Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2008 Proceedings

International Conference on Information Systems (ICIS)

2008

Are Markets for Vulnerabilities Effective?

Sam Ransbotham
Boston College, sam.ransbotham@bc.edu

Sabyasachi Mitra
Georgia Institute of Technology - Main Campus, saby.mitra@mgt.gatech.edu

Jon Ramsey
SecureWorks, Inc., jramsey@secureworks.com

ARE MARKETS FOR VULNERABILITIES EFFECTIVE?

Le marché des failles de sécurité est-il efficace?

Completed Research Paper

Sam Ransbotham
Boston College
Chestnut Hill, MA
sam.ransbotham@bc.edu

Sabyasachi Mitra
Georgia Institute of Technology
Atlanta, GA
saby.mitra@mgt.gatech.edu

Jon Ramsey
SecureWorks, Inc.
Atlanta, GA
jramsey@secureworks.com

Abstract

Security vulnerabilities are inextricably linked to information systems. Unable to eliminate these vulnerabilities, the security community is left to minimize their impact. Unfortunately, current reward structures may be skewed towards benefiting nefarious usage of vulnerability information rather than responsible disclosure. Recently suggested market-based mechanisms offer some hope by providing incentives to responsible security researchers. However, concerns exist that any benefits gained through increased incentives may be more than lost through information leakage. Using two years of security alert data, we examine the effectiveness of market-based mechanisms. While market-mechanisms do not reduce the likelihood that a vulnerability will be exploited, we find evidence that markets increase the time to vulnerability exploit and decrease the overall volume of alerts.

Keywords: Information security/privacy, IS policy, Vulnerability disclosure

Résumé

Les failles de sécurité sont inextricablement liées aux systèmes d'information. Celles-ci étant difficiles à éliminer, le service de sécurité a pour but de minimiser leur impact. Les mécanismes basés sur le marché apportent un espoir en attribuant des primes aux chercheurs chargés d'assurer la sécurité. Utilisant deux ans de données d'alerte, nous avons la preuve que les marchés favorisent au contraire l'exploitation des failles et diminuent le volume d'alertes.

Introduction

The unfortunate reality of widespread security vulnerabilities in technology products is an important topic not only to security and information systems professionals but also to consumers, business and policy makers. Modern commerce depends on information systems, yet security vulnerabilities pose ever-present risks which are no longer isolated to technical staff. In fact, policy aspects are increasing important as "incentives are becoming as important as technical design" (Anderson and Moore 2006, p. 610). Much of the incentive debate has focused on the discovery and disclosure of vulnerabilities and the associated incentives for provision of research effort towards discovery.

The security community relies on the others in the community to disclose vulnerabilities when found. Historically, researchers have not been directly compensated for their efforts in discovering vulnerabilities. In this sense, vulnerability research can be considered a public good—consumption of security information does not preclude others from using the information as well. Like other public goods, without additional incentives, security will be insufficiently provided (Garcia and Horowitz 2007). Therefore, vulnerability markets have been proposed to encourage researchers to provide this public good (Schechter 2004). Several private vulnerability markets are currently in existence, including iDefense and the Zero Day Initiative (ZDI). Summarizing data from the National Vulnerability Database, iDefense and ZDI, Figure 1 depicts the percentage of vulnerability disclosures made through a market mechanism for each year since 2000. While market disclosures remain a small fraction of the total disclosures, the markets are being increasingly used. So far in 2008, disclosures through market mechanism have leapt to 14% of the total disclosures.

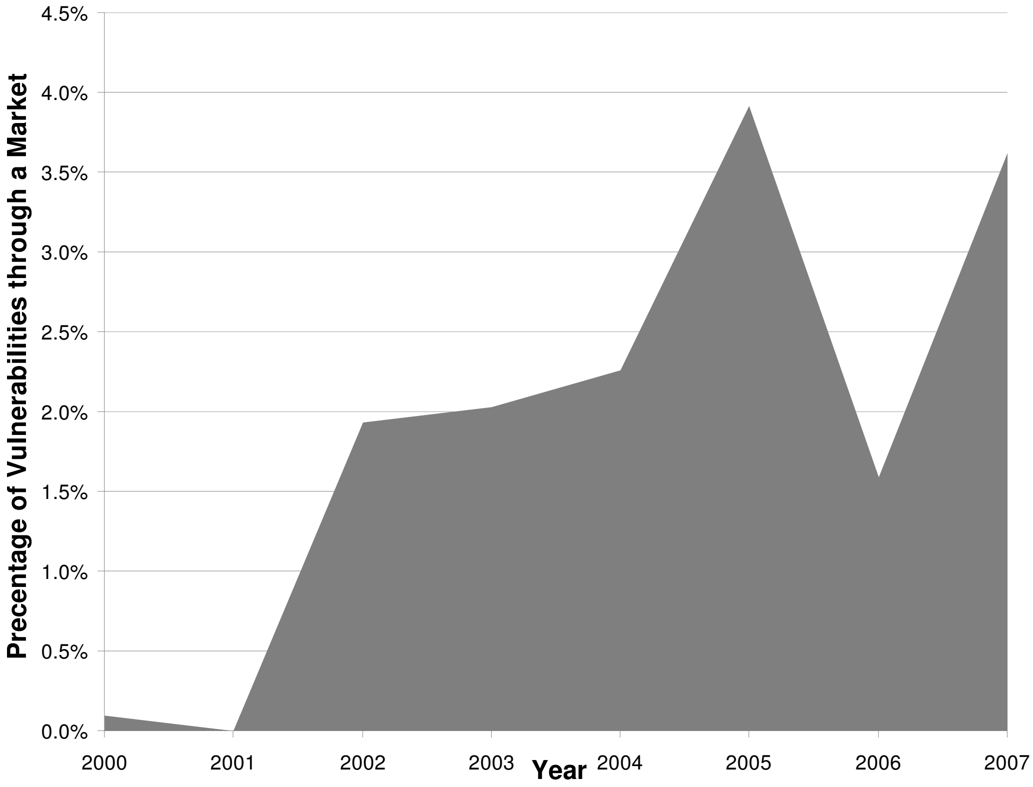

Figure 1: Percentage of Vulnerabilities Reported through a Market Mechanism

Despite their increased use, the impact of such markets is far from clear. By providing compensation for research, more effort should be expended. Yet, while markets create incentives for research and discovery, they have drawbacks. Because the private vulnerability markets focus on their own profit maximizing strategy, they have an incentive to leak vulnerability information and therefore decrease social welfare (Kannan and Telang 2005). Private vulnerability markets can increase the value for subscribers to their services by increasing the risks and penalties to non-subscribers. Thus, rather than having the desired effect of increasing security, they may instead be contributing to an overall decrease in security.

Thus, the fundamental question remains open—"are markets for vulnerabilities effective?" Our research addresses this question through a large scale empirical study of vulnerabilities disclosed through both market and non-market mechanisms. To gauge effectiveness, we examine three measures of effectiveness.

- **Risk** Does market disclosure affect the likelihood of a vulnerability being exploited?
- **Speed** Does market disclosure affect the speed of exploitation of a vulnerability?

- **Volume** Does market disclosure affect the volume of attacks based on the vulnerability?

We use real alert data from intrusion detection systems. Notifications, called alerts, are generated by intrusion detection systems when a data pattern is seen that is consistent with the data pattern from a vulnerability. Through the empirical study of more than 2.4 billion alerts generated from 2006 and 2007, we provide evidence that markets for vulnerabilities can be effective. First, while the overall exploitation of vulnerabilities is the same for market and non-market mechanisms, market based disclosures decrease the likelihood that the vulnerability will be exploited quickly. This allows more time for the security community to defend against the exploit through patching or developing countermeasures. Second, we find that market disclosure reduces the volume of alerts resulting from a vulnerability.

Disclosure Environment

Vulnerabilities exist in all systems whether they are known or unknown. Of the unknown vulnerabilities, there are two methods that a vulnerability can be discovered—labeled *malevolent* and *benign*. The defining distinction between the malevolent researcher and the benign researcher is their action upon discovery of the vulnerability. Figure 2 depicts the relationships between the sets of vulnerabilities.

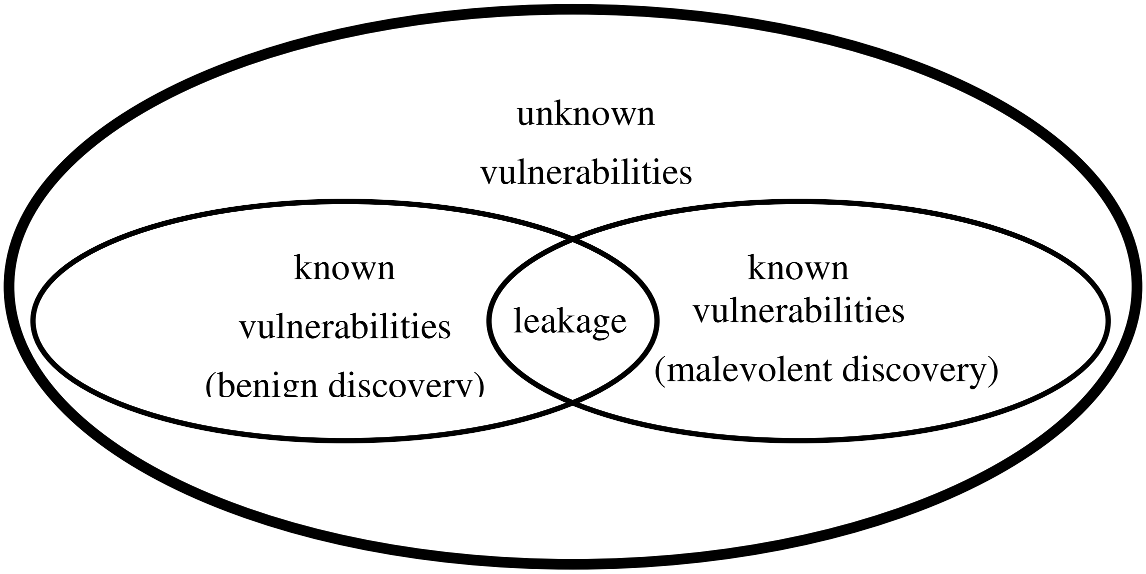
unknown vulnerabilities
known vulnerabilities (benign discovery)
leakage
known vulnerabilities (malevolent discovery)

Figure 2: Discovery of Vulnerabilities

First, a vulnerability can be found by a malevolent researcher. This researcher is rewarded through exploiting the vulnerability (or, alternatively, selling the vulnerability to others who will exploit the vulnerability.) The total value of this reward is the expected value of the sum of the successful exploitations of the vulnerability. In the case of malevolent discovery, the discover benefits most if the vulnerability is kept secret and also is not discovered by a benign researcher. Second, a vulnerability can be found by a benign researcher. With market mechanisms, the researcher is paid a reward by the market for their effort. (Without the market mechanism, there is no explicit monetary reward.)

These methods work independently, but are related. Benign researchers can find vulnerabilities that malevolent researchers have not found. However, to be useful for protection, a benign discoverer must use the vulnerability information. Leakage occurs when malevolent researchers learn of the vulnerability through usage. This leakage may be intentional, as private markets have incentives to leak information and increase the value of their services (Kannan and Telang 2005) or it may occur inadvertently through reverse engineering of protection systems. The inadvertent leakage is of particular concern. While reputation effects may discourage intentional leakage, inadvertent leakage is a by product of providing protection by using information about the discovered vulnerability.

Similarly, malevolent researchers may find vulnerabilities that benign researchers have not already found. In parallel to leakage of benign findings, the malevolent researcher must use the vulnerability to realize value. Usage of the vulnerability in an exploit may increase the likelihood of benign discovery.

Literature Review

Research is active in understanding the underlying economics of information security. Earlier work focused on topics such as risk management (Straub and Welke 1998), and handling abuse (Straub and Nance 1990). More recently, (Anderson and Moore 2006) and (Gordon and Loeb 2006) provide overviews of the key complexities surrounding the misaligned incentives, negative externalities, and general challenges for information systems professionals. Patching issues such as user incentives (August and Tunca 2006), restricted distribution (Rahman et al. 2006), and piracy (August and Tunca 2008) have been of recent research interest.

Recognizing that vulnerabilities are inevitable, research surrounding disclosure of vulnerabilities has been particularly active. While disclosure announcements can affect the value of software vendor (Telang and Wattal 2007), public disclosure can, under some conditions, promote social welfare (Nizovtsev and Thursby 2007). Further, disclosure itself has several options, each of which has their own strengths and weakness (Arora et al. 2004), particularly regarding the pressure that disclosure places on vendors. An importation variation in disclosure policy is the time given to vendors for correction prior to public disclosure. Vendors have been shown empirically to respond to disclosure (Arora et al. 2005) especially under certain competitive conditions (Arora et al. 2006a). Disclosure and patching has also been found to affect the volume of attacks observed in controlled research networks called *honeypots* (Arora et al. 2004; Arora et al. 2006b) However, while there is great value in the controlled environment that honeypots provide, our research is among the first empirical analysis using real, multi-firm alert data.

A significant issue in information systems security is the incentives for investment. Research has shown that security can be considered a public good and tends to be under-provisioned (Garcia and Horowitz 2007). The investment in IT security deterrence has been shown to be effective within a firm (Straub 1990). However, because of externalities, underinvestment is likely and regulation has been suggested to improve social welfare but faces significant challenges (Garcia and Horowitz 2007).

As an alternative, market mechanisms have been proposed to address the underinvestment. Specifically, rather than depending on the security community to freely contribute vulnerability research, payments can be used to encourage research (Schechter 2004). This approach recognizes the reward structure for vulnerabilities available in the black market (Radianti and Gonzalez 2007) and seeks to offset it. These markets for vulnerabilities have been suggested as an interesting economic model for exploration (Anderson and Moore 2006; Sutton and Nagel 2006). In addition to straight payment structures, auctions have been proposed but they, along with markets, have implementation difficulties (Ozment 2004). In fact, a recent vulnerability auction has been implemented (WabiSabiLabi). Yet, interest in market mechanisms remains the most active with two markets (iDefense and the Zero Day Initiative) in active use over the past couple of years.

The impact of such markets is not clear. The presence of private infomediaries introduces additional complexity to the disclosure and patch cycle (Li and Rao 2007). A specific concern is that markets have an incentive to leak information. In an analytical model, Kannan and Telang (2005) have shown that markets can reduce social welfare due to information leak. Further, the information leak does not have to be intentional by the markets. Instead, by reverse engineering signatures on intrusion detection systems, markets providing protection to their clients can inadvertently disclose vulnerabilities. Adding further complexity, Kumar et al. (2007) find differential effects from different types of information leaks such as vulnerabilities which reveal confidential information. In an abstract sense, much like there are concerns that weapon buyback programs may actually increase the number of guns (Mullin 2001), vulnerability purchase programs may increase the number of vulnerabilities.

Further complicating the analysis is that reward mechanisms have two effects (Cavusoglu et al. 2007). First, the rewards themselves encourage early discovery. Second, the reward markets provide their information only to a group of subscribing users. Using analytical models, Cavusoglu et al. (2007) show that early discovery does improve welfare, but providing information only to subscribing users does not necessarily improve welfare. Given that existing market mechanisms combine these two effects, it is not clear if social welfare is increased or decreased by the presence of these markets.

Overall, the effects of markets for vulnerabilities are ambiguous as increased incentives may be offset by information leakage. To examine the effectiveness of markets for vulnerabilities, we consider three possibilities.

- Does disclosure through a market mechanism affect the likelihood of a vulnerability being exploited?
- Does disclosure through a market mechanism affect the speed by which a vulnerability is exploited?
- Does disclosure through a market mechanism affect the volume of alerts issued from a vulnerability?

First, not all vulnerabilities disclosed are exploited. Attackers may find some vulnerabilities more attractive or more rewarding than others. One measure of effectiveness of a market would be if vulnerabilities disclosed through the market were more or less likely to be exploited. Based on the preceding concerns about leakage of information from the markets found in prior modeling (Kannan and Telang 2005), we hypothesize that:

> ***Hypothesis 1A:*** Disclosure through market mechanisms will *increase* the likelihood that a vulnerability will be exploited.

Most of the prior analysis of vulnerability disclosure is rooted in analytical economic modeling. However, the sociology and criminology literature can also provide other perspectives on crime and its societal context (Braithwaite 1989; Cohen and Felson 1979; Gottfredson and Hirschi 1990). While less precise than the rational choice models of crime in the economics literature (Ehrlich 1996), these theories depict a broader perspective on the causes and consequences of crime. A comprehensive review of this literature clearly is beyond the scope of this paper. Instead, we focus on the relevance of the traditional theories in the context of the market for vulnerability disclosures studied in this paper.

Criminal behavior is learned through association and social interaction with others, as in Differential Association theory (Sutherland 1947), the theory of Social Learning (Akers et al. 1979), or the Subculture of Delinquency theory (Cohen 1955). Labeling of individuals as deviants reinforces this behavior. Attackers and security professionals are separate groups with distinct subcultures reinforced through differential association and social learning. Responsible disclosure appeals to security professionals, but not to attackers whose subculture is likely to view reporting to a mainstream agency as unacceptable. Therefore, it is unlikely that changes to incentives will transform significant numbers of malevolent researchers into benign researchers.

However, Routine Activities theory views motivated offenders, suitable targets and the absence of capable guardians as pre-requisites of crime (Cohen and Felson 1979). Crime decreases with target hardening or with increasing negative consequences. While there will always be motivated offenders, hardening of targets through wide patching of vulnerabilities will lower the probability of successful compromise and consequently reduce the incentives for the attacker, who moves on to exploit other vulnerabilities. Thus, shifting the incentives for discovery not only changes researcher motivation, it has the secondary effect of changing the potential reward for attackers. Therefore, a contrasting hypothesis is:

> ***Hypothesis 1B:*** Disclosure through market mechanisms will *decrease* the likelihood that a vulnerability will be exploited.

Second, there are several potential advantages of disclosure through the market-based mechanisms based from information sharing among benign researchers. For example, vendors may be allowed adequate time to develop patches to correct the vulnerability, and users are given adequate time to deploy the patches. With this hardening of the target, attacks are less likely to be successful for vulnerabilities disclosed through the market mechanisms. Further, as more systems are patched within the universe of all systems, vulnerabilities that rely on propagation through affected systems are also rendered less effective (August and Tunca 2006; August and Tunca 2008). Consequently, the expected economic benefits from vulnerability exploitation are reduced, and attackers expend less energy in exploiting the vulnerability (Ehrlich 1996). Since the discovery mechanisms of markets may get information to the defenders more quickly, it can increase the time available for the deployment of countermeasures. Accordingly, we hypothesize that:

> ***Hypothesis 2:*** Disclosure through market mechanisms will *decrease* the likelihood that a vulnerability will be exploited soon after the vulnerability is published.

Third, the discovery of vulnerabilities through markets may decrease the usage of the vulnerability by attackers by the preceding reasoning. Since many of the vulnerabilities reported in non-market-based mechanisms are first exploited by attackers and then discovered by security professionals, these vulnerabilities are more likely to be exploited widely, leading to a greater volume of attacks. In summary, proactive discovery of vulnerabilities and private disclosure to vendors lowers propagation of attacks through affected systems and thereby reduce the overall volume of exploits. Therefore, we hypothesize that:

> ***Hypothesis 3:*** Disclosure through market mechanisms will *decrease* the number of alerts that are issued for a vulnerability.

Table 1: Sample Descriptive Statistics

Variable		**Percentage**	**Count**
Total		100.00%	13,249
	Market	2.60%	345
	Non-Market	97.40%	12,904
Access	Requires local computer access for exploitation	9.53%	1,262
	Requires adjacent access for exploitation	0.44%	58
	Requires only network access for exploitation	90.04%	11,929
Complexity	Low complexity	62.84%	8,326
	Medium complexity	29.41%	3,897
	High complexity	7.74%	1,026
Authentication	Not required	93.52%	12,391
	Required	6.48%	858
Confidentiality Impact	No disclosure of confidential information	28.30%	3,750
	Yes, disclosure of confidential information	71.70%	9,499
Integrity Impact	No impact on integrity of information	21.40%	2,835
	Yes, impact on integrity of information	78.60%	10,414
Availability Impact	No impact on availability of services	28.40%	3,763
	Yes, impact on availability of services	71.60%	9,486
Vulnerability	Access: incorrect escalation of privileges	4.95%	656
	Input: failure to handle input data correctly	51.13%	6,774
	Design: short comings in the design	11.85%	1,570
	Exception: failure to handle exceptional states	5.35%	709
	Environmental: historical, depends on setup	0.24%	32
	Configuration: improper configuration	0.87%	115
	Race Condition: failure to sequence events	0.62%	82
	Other	1.05%	139
Contains Signature	No	97.28%	12,888
	Yes	2.72%	361
Patch Available	No	66.89%	8,862
	Yes	33.11%	4,387

Data and Methodology

Data

To investigate the effectiveness of market mechanisms, our primary datasource is a summarized database of alerts generated from intrusion detection systems. An intrusion detection system (IDS) is installed to protect a network by filtering bad or potentially bad traffic from getting into the network. One way that an IDS works is by looking for sequences of data in a packet that match a known sequence associated with a vulnerability. These known sequences are called *signatures*. The basic role and function of intrusion detection systems are described in more detail in Cavusoglu et al. (2005) and Ransbotham and Mitra (2008). Each time a signature is observed, an alert is generated and saved for further analysis. The alert database is provided by SecureWorks, a managed security service provider. The dataset provides a unique forum for research analysis both because it contains real alert data (as opposed to data from a research setting) and because the data is from several thousand clients across many industries. These characteristics allow us to examine the actual effectiveness of markets using real data that is not specific to any single client. Unfortunately, real world IDS detection is imperfect, particularly in that it produces false positives due to incorrect signatures or configuration. Signatures may also be refined over time as the SecureWorks operators observe alerts. For the signatures in our final analysis, we verified with SecureWorks that both these focal signatures and focal IDS devices did not experience any significant abnormal adjustments. However, the dataset may still contain unknown false positives. The analysis is based on a summarized set of alerts from 2006 and 2007.

The key variable of interest is whether or not a vulnerability was disclosed through a market mechanism or through a non-market mechanism. During 2006 and 2007, there were two markets providing incentives for researchers to discover and disclose vulnerabilities through their service (iDefense and the Zero Day Initiative). During that same period, there were many other options which did not reward researchers directly. The most common of these are the CERT, Security Focus, XForce, Secunia, Bugtraq and Internet Security Systems X-Force. We include an indicator variable, *Market*, if a vulnerability was disclosed through one of the two market mechanisms.

Control Variables

We match the signatures for a vulnerability with the detailed information available primarily through the National Vulnerabilities Database (NVD 2008). Each vulnerability in the National Vulnerabilities Database (NVD) is assessed using a Common Vulnerability Scoring System (CVSS). Through this uniform scoring, we are able to control for specific attributes of the vulnerability. Details on Version 2 of the scoring system are in Mell and Romanosky (2008). From the scoring, we include the following:

- **Access Required:** This metric describes the proximity required to exploit the vulnerability. Proximities are scored as *local* if the attacker must have local access to the potential target, *adjacent* if attacker must be closely located or *remote* if the attacker can be across a non-local network.
- **Complexity:** Once the attacker has access, vulnerabilities have varying degrees of complexity to exploit and are categorized as *low*, *medium*, or *high* complexity. We include this characteristic because a more complex vulnerability may be more difficult to exploit and, if tied to a specific disclosure mechanism in an unobservable way, would not measure the market effectiveness.
- **Authentication Required:** Some vulnerabilities may be exploited anonymously; others require authentication. We include an indicator if the attacker must pass some authentication step to exploit the vulnerability. While the CVSS indicates the number of authentications required (either *None*, *Single*, or *Multiple*), we use an indicator variable *Authentication Required* if any authentication is required due to a low number of multiple authentication vulnerabilities reported.
- **Impact:** The potential impact of a vulnerability is categorized as affecting the disclosure of confidential information (*Confidentiality*), the integrity of data (*Integrity*) or the availability of system resources (*Availability*). For each, the CVSS reports impacts of None, Partial, or Complete. However, we use an indicator variable for each category if the impact is present. (There are few partial impact vulnerabilities.)

Beyond the scoring, there are other aspects of the vulnerability for which we are able to control. First, the NVD includes seven different types of vulnerabilities. They are incorrect allowance of privileges (*Access Validation*), failure to handle incorrect input (*Input Validation*), shortcomings in design of software (*Design Error*), insufficient response to unexpected conditions (*Exception Error*), weak configuration of settings (*Configuration Error*), errors due to sequencing of events (*Race Condition*), or uncategorized (*Other*). Indicator variables are included for these categories. Second, we include an indicator variable, *Patch Available*, if a patch was available at the time that the vulnerability was disclosure. Next, we include an indicator variable, *Signature Available*, if a signature was available at the time that the vulnerability was disclosed. Further, we also include the age of vulnerability measured as the number of days since the vulnerability was disclosed. Finally, in several of the following analyses, we are also able to control for changes in trends over time using fixed effects.

Table 2: Selection of Market or Non-Market Disclosure

Variable	**Model 0**	**Model 1**	**Model 2**	**Model 3**	**Model 4**	**Model 5**	**Model 6**
Constant	-5.9814***	-1.8711***	-5.9938***	-5.9888***	-7.1940***	-5.1101***	-5.9267***
	(1.0013)	(0.2383)	(1.0024)	(1.0015)	(1.0137)	(1.0052)	(1.0267)
Access: Adjacent		-0.0252					-0.0783
		(0.4732)					(0.4897)
Access: Network		-1.1539***					-0.8516***
		(0.1333)					(0.1526)
Complexity: Medium			0.0273				0.3057**
			(0.1207)				(0.1331)
Complexity: High			0.2623				0.1256
			(0.2311)				(0.2398)
Authentication				0.1694			-0.3179
				(0.2001)			(0.2165)
Confidence Impact					0.5191***		0.6293***
					(0.2037)		(0.2127)
Integrity Impact					-0.1333		0.2080
					(0.1966)		(0.2148)
Availability Impact					1.2411***		0.8335***
					(0.2032)		(0.2097)
Vuln: Access						-0.6798***	-0.6842***
						(0.2542)	(0.2547)
Vuln: Input Validation						-1.9849***	-1.7928***
						(0.1676)	(0.1757)
Vuln: Design						-0.7530***	-0.6565***
						(0.1966)	(0.2029)
Vuln: Exception						-0.2745	0.1371
						(0.2129)	(0.2153)
Vuln: Config						-1.0329	-1.1215
						(0.7379)	(0.7343)
Vuln: Race						0.2214	-0.1099
						(0.4560)	(0.4733)
Vuln: Other						-1.0338**	-0.9215*
						(0.5269)	(0.5282)
Fixed Effects	month	month	month	month	month	month	Month
Log likelihood	-1525.252	-1492.871	-1524.638	-1524.915	-1486.892	-1426.771	-1377.621
Pseudo R^2	4.62	6.64	4.65	4.64	7.02	10.73	13.80
Wald χ^2	110.23***	180.77***	110.03***	111.95***	183.13***	278.89***	378.67***

Logit model (Dependent variable is 1=market, 0= non-market), robust standard errors in parenthesis.
Two-tailed significance: * (p<0.10); ** (p<0.05); *** (p<0.01). n = 13,249

Methodology

First, in our sample of 1252 vulnerabilities for which we had full data with alert signatures matched into the NVD database, only 153 (12%) were exploited by attackers. To examine the difference that market disclosure makes in the likelihood of exploitation, we use the logit regression $\ln\left(e_i \big/ (1-e_i)\right) = \beta x_i + \beta_{market} x_{market,i}$. The variable e_i takes the value of 1 when an exploit of vulnerability i is observed. Vector β is the vector of control variables listed in the previous section and variable $x_{market,i}$ is 1 if the market mechanism for disclosure was used. Further, because of the potential for censoring caused by the end of the study, we use a Cox proportional hazard model (Cox 1972) to provide further support. In the proportional hazard model, the risk of failure (exploitation of a vulnerability) at time t for vulnerability i is given by $\lambda(t) = \lambda_0(t_i)\, e^{-x_i \beta}$. These analyses allow an empirical answer to the competing hypotheses that markets either increase or decrease the likelihood of exploitation of a vulnerability (Hypothesis 1A and Hypothesis 1B).

Second, we use another logit model to examine the risk of exploitation shortly after the vulnerability is published. The risk of exploitation in the prior analysis only evaluated the risk of exploitation during the entire study period. For comparison, we use similar logit regression to determine the risk of exploitation within one month and one week of disclosure. This analysis allows an empirical answer to the hypothesis that markets decrease the likelihood that an exploit will be observed soon after disclosure (Hypothesis 2).

Third, we built a panel dataset which contains the daily count of alerts for each type of vulnerability for the period from 2006 to 2007. By summarizing the 2.4 billion alerts into daily counts, our sample size is reduced to a tractable number for analysis. The sample is then further reduced by the alerts for which we found matching information in the NBD. We use a random effects panel regression to estimate the impact of market disclosure on the natural log of the number of alerts, $a_{i,t}$ for vulnerability i. The model estimated is $\ln(a_{i,t}) = x_{i,t}\, \beta + \alpha_i + u_{i,t}$ where $x_{i,t}$ is the vector of control variables, α_i are the random effects, and $u_{i,t}$ is the error term. This analysis allows an empirical answer to the hypothesis that markets decrease the overall volume of alerts generated (Hypothesis 3).

Selection of Disclosure to Market or Non-Market

Before examining the effectiveness of the market mechanisms, we first compare the vulnerabilities disclosed through the two mechanisms. For this comparison, we use the entire set of vulnerabilities contained in the NVD.

While there are several repositories of vulnerability information, the NVD contains a large cross sections of vulnerabilities consistently reported. Similar large scale analysis have been done of vulnerabilities (Frei et al. 2006), but have not focused on the selection of disclosure mechanism. During 2006 and 2007, the NVD published information about 13,249 vulnerabilities. Of these, 345 (2.6%) were initially reported by one of the two market mechanisms. Table 1 shows descriptive statistics about all of the vulnerabilities disclosed during 2006 and 2007.

We use a logit model to analyze the selection of disclosure through the market or non-market mechanism. Table 2 shows the influence of vulnerability attributes on the likelihood of being disclosed through a market mechanism versus a non-market mechanism. The logit analysis indicates that vulnerabilities which only require network access are associated with non-market disclosure. Similarly, vulnerabilities based on access violation, input validation errors, and design omissions are also associated with non-market disclosure. Conversely, market disclosures are associated vulnerabilities of medium complexity or which impact system confidence or availability. The log likelihood and Wald χ^2 indicate that the model is a good fit and, although the pseudo-R^2 is an incomplete measure, does explain some of the variance. Overall, the analysis suggests that there are distinct associations between some vulnerability attributes and resultant disclosure mechanism.

Table 3 shows a similar analysis to Table 2, but examines changes in attribute influence through 2006 to 2007. Based on the logit analysis, none of the explanatory variables shift their influence from market to non-market during the time period. However, the magnitude of some of the coefficients changes significantly. For example, while vulnerabilities which require only network access (instead of local access) to exploit are consistently more often reported through non-market mechanisms, their association with non-market disclosure increases in strength during the period of the study. Also, which input validation based vulnerabilities are initially strongly associated with non-market disclosure in early 2006, by the end of 2007, they are as likely to be disclosed though one mechanism as the other. Overall, this suggests there are some minor changes in the attributes of vulnerabilities which are being disclosed through each type of mechanism.

Table 3: Selection of Market or Non-Market Disclosure Over Time

Variable	Jan-Jun 2006	Jul-Dec 2006	Jan-Jun 2007	Jul-Dec 2007
Constant	-4.9775*** (0.9244)	-3.9975*** (0.6021)	-3.3216*** (0.5055)	-3.9254*** (0.4265)
Access: Adjacent	—	—	0.9347 (0.6304)	-0.0201 (1.1797)
Access: Network	-0.7876* (0.4640)	-0.6035* (0.3343)	-0.3068 (0.2776)	-1.4280*** (0.2437)
Complexity: Medium	1.2863 (0.8560)	0.3036 (0.3605)	0.2694 (0.1947)	0.3071 (0.2115)
Complexity: High	0.1003 (0.5322)	0.1407 (0.3743)	0.0909 (0.4728)	0.0458 (0.6339)
Authentication	-0.2378 (0.8243)	0.4300 (0.3512)	-0.4736 (0.3586)	-0.7969* (0.4677)
Confidence Impact	1.0001 (0.8318)	0.4754 (0.4759)	0.2709 (0.3581)	1.0937*** (0.3482)
Integrity Impact	0.1989 (0.8843)	-0.2622 (0.4731)	0.4775 (0.3766)	0.5036 (0.3699)
Availability Impact	1.3898* (0.7941)	1.2638*** (0.4660)	0.5847* (0.3453)	0.6368* (0.3579)
Vuln: Access	-1.2168 (0.9957)	-0.9925 (0.7308)	-0.3530 (0.3133)	-0.4414 (0.7252)
Vuln: Input Validation	-2.7317*** (0.7664)	-1.3152** (0.3198)	-2.0968** (0.2775)	-0.4571 (0.3176)
Vuln: Design	-1.3637** (0.6355)	-0.1658 (0.3873)	-0.7064** (0.2972)	0.0125 (0.4022)
Vuln: Exception	-0.0785 (0.6864)	0.3863 (0.3977)	0.0828 (0.3115)	0.3608 (0.6182)
Vuln: Race	0.4436 (1.1025)	—	0.3627 (0.6664)	0.1672 (0.7678)
Vuln: Other	—	0.5145 (1.1557)	—	0.2072 (0.6116)
Vuln: Config	—	—	-0.5226 (1.0262)	-0.2785 (1.2070)
Observations	3112	3381	3574	2980
Log likelihood	-139.26106	-335.76698	-485.92231	-433.99179
Pseudo R^2	17.65	7.65	11.42	9.09
Wald χ^2	110.23***	75.18***	113.78***	98.92***

Logit model (dependent variable is 1=market, 0= non-market), robust standard errors in parenthesis.

Two-tailed significance: * (p<0.10); ** (p<0.05); *** (p<0.01). n = 13,249

Table 4: Choice of Exploitation of Vulnerabilities

	Within Sample		Within One Month		Within One Week	
Variable	**Model 1**	**Model 2**	**Model 3**	**Model 4**	**Model 5**	**Model 6**
Constant	-2.3932***	-2.3716***	-4.1762***	-4.1280***	-3.2629***	-3.1895
	(0.3871)	(0.3842)	(0.6517)	(0.6466)	(0.7053)	(0.7018)
Complexity: Medium	-0.9509***	-0.9468***	-0.7935**	-0.7877**	-1.1818***	-1.2041***
	(0.2368)	(0.2366)	(0.3248)	(0.3261)	(0.4789)	(0.4837)
Complexity: High	0.1557	0.1494	0.3835	0.3735	0.5078	0.4738
	(0.2614)	(0.2620)	(0.3233)	(0.3236)	(0.4342)	(0.4367)
Confidence Impact	0.3541	0.3566	0.2254	0.23821	-1.5491**	-1.5984**
	(0.3048)	(0.3048)	(0.5327)	(0.5342)	(0.6785)	(0.7135)
Integrity Impact	0.9716***	0.9706***	1.4507**	1.4515**	—	—
	(0.3238)	(0.3227)	(0.6129)	(0.6115)		
Availability Impact	-0.2330	-0.2287	0.2674	0.2682	1.3606*	1.4296*
	(0.2605)	(0.2590)	(0.4763)	(0.4723)	(0.7424)	(0.7740)
Vuln: Access	-0.8830	-0.8600	-0.7107	-0.6484	0.3110	0.4770
	(0.7604)	(0.76128)	(1.0447)	(1.0470)	(1.1211)	(1.1406)
Vuln: Input Validation	0.4081**	0.3894*	0.3344	0.2913	0.9179***	0.8800***
	(0.2069)	(0.2054)	(0.2664)	(0.2632)	(0.3551)	(0.3555)
Vuln: Design	-0.0996	-0.1259	0.2170	0.1520	0.1777	0.0723
	(0.2946)	(0.2943)	(0.3773)	(0.3769)	(0.5332)	(0.5299)
Vuln: Exception	-0.1688	-0.1923	-0.7212	-0.7923	-0.4856	-0.6495
	(0.3856)	(0.3848)	(0.6391)	(0.6402)	(0.8335)	(0.8475)
Vuln: Config	0.5444	0.5410	-0.0297	-0.0460	—	—
	(0.6993)	(0.7073)	(1.0526)	(1.0555)		
Vuln: Race	-0.3283	-0.3260	—	—	—	—
	(0.9724)	(0.9537)				
Vuln: Other	-0.0101	-0.0512	0.8282	0.7252	0.1974	0.0002
	(0.7050)	(0.7058)	(0.7301)	(0.7308)	(1.2151)	(1.2061)
Patch Available	-0.5976***	-0.5701***	-0.4687*	-0.4074	-0.4770	-0.3960
	(0.1871)	(0.1917)	(0.2596)	(0.2641)	(0.3706)	(0.3720)
Signature Available	1.1066***	1.1228***	1.2743***	1.3161***	2.1340***	2.2411***
	(0.2412)	(0.2413)	(0.2984)	(0.3000)	(0.3996)	(0.4056)
Market Disclosure		-0.2598		-0.6691		-1.3421*
		(0.3089)		(0.4507)		(0.7609)
Observations	1055	1055	1047	1047	804	804
Log likelihood	-397.2295	-396.8439	-239.6904	-238.4691	-132.3755	-130.2724
Pseudo R^2	9.05	9.14	10.36	10.82	15.17	16.52
Wald χ^2	70.91***	72.37***	52.28***	54.45***	52.85***	54.37***

Logit model (Dependent variable is 1=exploited, 0= non-exploited), robust standard errors in parenthesis.

Two-tailed significance: * (p<0.10); ** (p<0.05); *** (p<0.01).

Empirical Examination of Market Effectiveness

First, we examine how market or non-market disclosure affects the risk of the vulnerability being exploited. The logit regressions in Model 1 and Model 2 (Table 4) indicate that disclosure through a market mechanism does not significantly affect the likelihood of a vulnerability being exploited. Interestingly, medium complexity vulnerabilities are less likely to be exploited than low complexity, but high complexity are not. Attackers also appear to be more likely to exploit vulnerabilities impacting system integrity. As expected, the availability of patches reduces the likelihood of exploit as attacker may feel that their chances of success are diminished. The availability of a signature increases the likelihood of exploitation providing some evidence that attackers gain information about how to exploit a vulnerability by examining a signature. Because the sample is censored at the end of 2007, the similar analysis was done using a proportional hazard model (Table 5). In both estimations, we see no evidence that market disclosure increases the likelihood that a vulnerability will be exploited.

Table 5: Risk of Exploitation of Vulnerabilities

	Complete Sample		**Within One Month**		**Within One Week**	
Variable	**Model 0**	**Model 1**	**Model 0**	**Model 1**	**Model 0**	**Model 1**
Complexity: Medium	1.3984 (0.3379)	1.4638 (0.3622)	2.1970** (0.8030)	2.5432** (1.0007)	3.1766*** (1.4843)	3.8307*** (1.9330)
Complexity: High	1.5224* (0.3636)	1.5025* (0.3616)	2.3322*** (0.7704)	2.2943*** (0.7626)	3.0749** (1.4226)	2.8543** (1.3638)
Confidence Impact	1.2940 (0.3951)	1.3229 (0.4066)	1.1187 (0.6510)	1.1713 (0.6981)	0.9751 (0.4746)	1.0393 (0.4953)
Integrity Impact	2.1233** (0.6877)	2.0968** (0.6798)	4.0060** (2.4923)	3.9278** (2.4886)	—	—
Availability Impact	0.8873 (0.2320)	0.8906 (0.2326)	1.3789 (0.7347)	1.4021 (0.7641)	2.0654 (1.1147)	1.9934 (1.1286)
Vuln: Access	0.3363 (0.2591)	0.3249 (0.2521)	0.4599 (0.5178)	0.4129 (0.4770)	1.1256 (1.3714)	0.8777 (1.1387)
Vuln: Input Validation	1.2037 (0.2453)	1.1858 (0.2404)	1.2414 (0.3682)	1.1759 (0.3487)	1.8313 (0.7413)	1.7122 (0.7048)
Vuln: Design	0.9082 (0.2666)	0.8900 (0.2604)	1.2300 (0.4986)	1.1580 (0.4713)	1.1447 (0.7084)	0.9937 (0.6318)
Vuln: Exception	1.1981 (0.4327)	1.1569 (0.4170)	0.8330 (0.5469)	0.7629 (0.5003)	0.8323 (0.7051)	0.7372 (0.6193)
Vuln: Config	1.3376 (0.7560)	1.3081 (0.7420)	0.7641 (0.9162)	0.7047 (0.8577)	—	—
Vuln: Race	0.3786 (0.3808)	0.3695 (0.3750)	—	—	—	—
Vuln: Other	1.0330 (0.9639)	0.9846 (0.9207)	1.9560 (1.9384)	1.7355 (1.7282)	1.9394 (2.5105)	1.5847 (2.0910)
Patch Available	0.4740*** (0.0924)	0.4800*** (0.0939)	0.4855 (0.1460)	0.4846** (0.1483)	0.6048 (0.2732)	0.6013 (0.2816)
Signature Available	2.3354*** (0.5133)	2.3783*** (0.5254)	3.0832** (0.953)	3.1719*** (1.0081)	5.2960*** (2.0603)	5.6997*** (2.3434)
Market Disclosure		0.7259 (0.2133)		0.4513* (0.2174)		0.2662* (0.2061)
Failures	153	153	74	74	39	39
Log likelihood	-859.405	-858.665	-380.595	-378.633	-189.239	-186.9790
Wald χ^2	49.86***	50.86***	2643.01***	2192.94***	6984.87***	5729.36***

Cox proportional hazard model; failure is exploitation of vulnerability, robust standard errors in parenthesis.
Two-tailed significance: * (p<0.10); ** (p<0.05); *** (p<0.01). Observations = 1252.

Based on these results, we find no support for Hypothesis 1A or Hypothesis 1B that markets increase or decrease the risk of exploitation.

Table 6: Volume of Alerts based on Market or Non-Market Disclosure

Variable	Model 0	Model 1	Model 2	Model 3	Model 4	Model 5
Constant	-0.4666* (0.2830)	-0.4980 (0.2805)	-0.4699 (0.3186)	-0.4784* (0.2816)	-0.4870* (0.2821)	-0.5252* (0.3163)
Access: Network	0.4205 (0.2608)	0.4120 (0.2580)	0.4223 (0.2652)	0.4606* (0.2591)	0.4636* (0.2606)	0.4933* (0.2619)
Complexity: Medium	-0.1359 (0.1229)	-0.0918 (0.1232)	-0.1358 (0.1230)	-0.1604 (0.1227)	-0.1017 (0.1220)	-0.0809 (0.1218)
Complexity: High	0.3640* (0.2155)	0.3559* (0.2156)	0.3638* (0.2157)	0.2801 (0.2174)	0.3523* (0.2153)	0.2614 (0.2173)
Authentication	-0.4927*** (0.0780)	-0.4908*** (0.0788)	-0.4929*** (0.0780)	-0.4461*** (0.0775)	-0.4827** (0.0772)	-0.4337*** (0.0776)
Confidence Impact	0.0560 (0.1912)	0.0505 (0.1911)	0.0560 (0.1914)	0.0156 (0.1905)	0.0608 (0.1907)	0.0157 (0.1896)
Integrity Impact	0.0568 (0.1929)	0.0454 (0.1926)	0.0561 (0.1894)	0.0542 (0.1921)	0.0896 (0.1938)	0.0779 (0.1891)
Availability Impact	0.0186 (0.1735)	0.0222 (0.1734)	0.0189 (0.1744)	-0.0226 (0.1744)	0.0211 (0.1730)	-0.0162 (0.1749)
Vuln: Access	0.0188 (0.1764)	0.0252 (0.1763)	0.0184 (0.1750)	0.0718 (0.1756)	0.0366 (0.1759)	0.0964 (0.1732)
Vuln: Input Validation	0.1068 (0.1375)	0.0975 (0.1376)	0.1071 (0.1394)	0.1105 (0.1367)	0.0651 (0.1382)	0.0577 (0.1389)
Vuln: Design	-0.0406 (0.1691)	-0.0347 (0.1694)	-0.0402 (0.1703)	-0.0781 (0.1693)	-0.0647 (0.1690)	-0.0972 (0.1704)
Vuln: Exception	-0.0288 (0.2933)	-0.0154 (0.2931)	-0.0296 (0.2948)	-0.1314 (0.2920)	-0.0180 (0.2931)	-0.1040 (0.2919)
Vuln: Config	-0.2393 (0.3600)	-0.2601 (0.3599)	-0.2380 (0.3633)	-0.1843 (0.3588)	-0.2412 (0.3591)	-0.2098 (0.3604)
Vuln: Race	0.2657 (1.2573)	0.2084 (1.2597)	0.2659 (1.2586)	-0.0669 (1.2710)	0.1940 (1.2552)	-0.1933 (1.2732)
Vuln: Other	-0.3946 (1.1531)	-0.3618 (1.1646)	-0.3927 (01.156)	-0.7191 (1.1582)	-0.4516 (1.1502)	-0.7435 (1.1696)
Age (ln)		0.0421*** (0.0055)				0.0419*** (0.0055)
Patch Available			0.0033 (0.1181)			-0.0053 (0.1206)
Signature Available				0.4224** (0.2081)		0.4160** (0.2100)
Market					-0.3179*** (0.1199)	-0.3287*** (0.1246)
Fixed Effects	month	month	month	month	month	month
Within R^2	1.22	1.26	1.22	1.22	1.22	1.26
Between R^2	2.95	3.44	2.95	4.56	3.9	5.9
Overall R^2	2.77	3	2.78	3.11	3.28	3.83
Wald R^2	1680.39***	1708.44***	1686.00***	1689.74***	1680.74***	1725.99***

Panel regression; dependent variable = log of the number of alerts; n = 139,347; 343 vulnerabilities
robust standard errors in parenthesis. Two-tailed significance: * (p<0.10); ** (p<0.05\$); *** (\$p<0.01\$).

Next, we examine how market or non-market disclosure affects the speed with which a vulnerability is exploited. The logit regressions in Model 3 and Model 4 (Table 4) indicate that disclosure through a market mechanism does not significantly affect the likelihood of a vulnerability being exploited within one month of disclosure. However, Model 5 and Model 6 do indicate that market disclosure decreases the likelihood of exploitation during the week after publication. (Similar models using time periods shorter than one week show similar results, but lack statistical power primarily due to the reduced number of exploitations in general as the time period shrinks.) This is important because decreasing the likelihood of exploitation in the short term allows for IT infrastructure professionals to implement countermeasures such as patching. Based on these results, we find support for Hypothesis 2 that markets decrease the risk of exploitation shortly after disclosure.

Finally, we examine the volume of alerts generated by a vulnerability. The panel regression in Table 6 is based on 139,347 daily observations of each vulnerability for 960 client locations. Model 1 shows that the volume of alerts increases as the age increases. Model 2 finds no evidence that the availability of a patch reduces the volume of alerts. Model 3 finds that the availability of a signature increases the volume of alerts. Finally, Model 4 and Model 5 show that disclosure through a market mechanism significantly reduces the volume of alerts issued. Based on these results, we find support for Hypothesis 3 that markets decrease the volume of alerts from a vulnerability.

Summary and Conclusions

Overall, the theoretical impact of market-based mechanisms for disclosure are not clear. While markets increase incentives for security research, they may have a negative impact due to the likelihood of information leakage (Kannan and Telang 2005). Based on a large scale empirical study of real alerts from intrusion detection systems across 960 clients for two years, we find evidence of market effectiveness.

First, while market disclosure does not increase or decrease the likelihood that a vulnerability will be exploited, it does decrease the likelihood of exploitation during the one week period after disclosure. This decrease is important for practitioners in that it allows more time to implement countermeasures. Further, it indicates that while leakage may happen, there are potentially positive aspects of leakage. Second, market disclosure does reduce the volume of alerts. Because of the overwhelming number of alerts, mechanisms which reduce the volume of alerts can help administrators better allocate resources.

In general, while information leakage may be occurring, the loss in welfare may be offset not only by incentive gains but also by positive aspects of leakage as others in the security community are made aware of vulnerabilities. This aspect points to opportunities for research to model and to quantify both the benefits and costs of information leakage. Future research could also help quantify the impact of specific incentive levels in increasing the vulnerabilities discovered. Research would also be valuable that helped understand if markets are truly providing incentives or are just compensating those would be researching and disclosing anyway.

Finally, the evidence of effectiveness is encouraging for both policy makers and the security community. Markets can be effective. Mechanisms that combine the incentive structures and positive aspects of information sharing while restricting the negative consequences of leakage could positively impact social welfare. It is towards these mechanism designs that our research provides encouragement.

References

Akers, R.L., Krohn, M., Lanza-Kaduce, L., and Radosevich, M. 1979. "Social Learning and Deviant Behavior: A Specific Test of a General Theory," American Sociological Review (44:4), August 1979, pp 636-655.

Anderson, R., and Moore, T. 2006. "The Economics of Information Security," Science (314:5799), pp 610-613.

Arora, A., Forman, C., Nandkumar, A., and Telang, R. 2006a. "Competition and Quality Restoration: An Empirical Analysis of Vendor Response to Software Vulnerabilities," Workshop on Information Systems and Economics.

Arora , A., Krishnan, R., Nandkumar, A., Telang, R., and Yang, Y. 2004. "Impact of Vulnerability Disclosure and Patch Availability—An Empirical Analysis," Workshop on the Economics of Information Security.

Arora, A., Krishnan, R., Telang, R., and Yang, Y. 2005. "An Empirical Analysis of Vendor Response to Disclosure Policy," Workshop on the Economics of Information Security.

Arora, A., Nandkumar, A., and Telang, R. 2006b. "Does Information Security Attack Frequency Increase with Vulnerability Disclosure? An Empirical Analysis," Information Systems Frontiers (8:5), pp 350-362.

Arora, A., Telang, R., and Xu, H. 2004. "Timing Disclosure of Software Vulnerability for Optimal Social Welfare," Third Workshop on Economics of Information Systems, Minneapolis, MN, pp. 1-47.

August, T., and Tunca, T.I. 2006. "Network Software Security and User Incentives," Management Science (52:11), pp 1703-1720.

August, T., and Tunca, T.I. 2008. "Let the Pirates Patch? An Economic Analysis of Software Security Patch Restrictions," Information Systems Research (19:1), pp 48-70.

Braithwaite, J. 1989. Crime, Shame and Reintegration. Cambridge, U.K.:

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. 2007. "Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge," IEEE Transactions on Software Engineering (33:3), pp 171-185.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2005. "The Value of Intrusion Detection Systems in Information Technology Security Architecture," Information Systems Research (16:1), March 2005, pp 28-46.

Cohen, A.K. 1955. Delinquent Boys: The Culture of the Gang. New York: Free Press.

Cohen, L.E., and Felson, M. 1979. "Social Change and Crime Rate Change: A Routine Activity Approach," American Sociological Review (44:4), August 1979, pp 588-608.

Cox, D.R. 1972. "Regression Models and Life Tables," Journal of the Royal Statistical Society, B (34), pp 187-202.

Ehrlich, I. 1996. "Crime, Punishment and the Market for Offences," Journal of Economic Perspectives (10:1), pp 43-67.

Frei, S., May, M., Fiedler, U., and Plattner, B. 2006. "Large-scale Vulnerability Analysis," Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense: ACM Press, pp. 131-138.

Garcia, A., and Horowitz, B. 2007. "The Potential for Underinvestment in Internet Security: Implications for Regulatory Policy," Journal of Regulatory Economics (31:1), pp 37-55.

Gordon, L.A., and Loeb, M.P. 2006. "Budgeting Process for Information Security Expenditures," Communications of the ACM (49:1), p 121.

Gottfredson, M.R., and Hirschi, T. 1990. A General Theory of Crime. Stanford: Stanford University Press.

Kannan, K., and Telang, R. 2005. "Market for Software Vulnerabilities? Think Again," Management Science (51:5), May 2005, pp 726-740.

Kumar, V., Telang, R., and Mukhopadhyay, T. 2007. "Optimally Securing Interconnected Information Systems and Assets," Workshop on the Economics of Information Security, Pittsburgh, PA.

Li, P., and Rao, H.R. 2007. "An Examination of Private Intermediaries' Roles in Software Vulnerabilities Disclosure," Information Systems Frontiers (9:5), pp 531-539.

Mell, P., and Romanosky, S. 2008. "A Complete Guide to the Common Vulnerability Scoring System Version 2.0", http://www.first.org/cvss/cvss-guide.html accessed 8 March 2008.

Mullin, W.P. 2001. "Will Gun Buyback Programs Increase the Quantity of Guns?," International Review of Law & Economics (21:1), pp 87-102.

Nizovtsev, D., and Thursby, M. 2007. "To Disclose or Not? An Analysis of Software User Behavior," Information Economics and Policy (19), pp 43-64.

NVD. 2008. "National Vulnerability Database", http://nvd.nist.gov/, accessed 23 April 2008.

Ozment, A. 2004. "Bug Auctions: Vulnerability Markets Reconsidered," Workshop on the Economics of Information Security.

Radianti, J., and Gonzalez, J.J. 2007. "Understanding Hidden Information Security Threats: The Vulnerability Black Market," 40th Annual Hawaii International Conference on System Sciences: IEEE Computer Society.

Rahman, M.S., Kannan, K., and Tawarmalani, M. 2006. "The Countervailing Incentive of Restricted Patch Distribution: Economic and Policy Implications," Workshop on the Economics of Information Security.

Ransbotham, S., and Mitra, S. 2008. "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," Information Systems Research (forthcoming).

Schechter, S. 2004. "Computer Security, Strength and Risk: A Quantitative Approach," Ph.D. Thesis, Harvard University

Straub, D. 1990. "Effective IS Security: an Empirical Study," Information Systems Research (1:3), 1990, pp 255-276.

Straub, D., and Nance, W. 1990. "Discovering and Disciplining Computer Abuse in Organizations: a Field Study," MIS Quarterly (14:1), 1990, pp 45-60.

Straub, D., and Welke, R. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," MIS Quarterly (22:4), December 1998, pp 441-469.

Sutherland, E. 1947. Principles of Criminology. Philadelphia: Lippincot.

Sutton, M., and Nagel, F. 2006. "Emerging Economic Models for Vulnerability Research," Workshop on the Economics of Information Security.

Telang, R., and Wattal, S. 2007. "An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price," IEEE Transactions on Software Engineering), pp 544-557.