The Deterrent and Displacement Effects of Information Security Enforcement: International Evidence

*Ivan P.L. Png** ipng@comp.nus.edu.sg
*Chen-Yu Wang** wangunited@hotmail.com
*Qiu-Hong Wang** wangqiuh@comp.nus.edu.sg

Abstract

We present two methodologies that adapt the event study from research in finance and economics to study the impact of enforcement on information security attacks. One uses linear regression with the number of attacks as the dependent variable and indicators of enforcement events as independent variables. The other measures the impact of enforcement by the difference between the actual and predicted number of attacks. We find limited evidence that domestic enforcement deters attacks within the country. However, we find compelling evidence of a displacement effect: U.S. enforcement substantially increases attacks originating from other countries. Our findings are robust to differences in the effective time window of enforcement.

1. Introduction

That government enforcement effectively deters criminal behavior is the central premise in analyses of crime in general [4] [20] and information security in particular [10] [13] [16] [19]. Early studies of the impact of enforcement on crime yielded inconclusive results [7]. Only relatively recently have empirical studies shown that increased enforcement does indeed reduce crime [5] [17].

However, information security is far removed from the crimes typically studied in the literature on the economics of enforcement – murder, assault, burglary, etc. Accordingly, the empirical question of whether enforcement deters computer attacks remains an important open question.

In this paper, we investigate this issue using a sample of attacks on 15 countries over the period January 2004 to June 2006. Our empirical strategy adapts the event study methodology which has been widely used in the disciplines of finance and economics. One uses linear regression with the number of attacks as the dependent variable and indicators of enforcement events as independent variables. The other measures the impact of enforcement by the difference between the actual and predicted number of attacks.

From a newspaper database and other public media resources, we identified 187 reports of enforcement action in 15 countries against information security violators during the sample period. We then measured the impact of those enforcement actions on the rate of information security attacks originating from the respective country. Since the United States is the largest source of information security attacks, we also investigated whether U.S. enforcement action might *displace* attackers to other countries. For instance, U.S. enforcement might induce perpetrators of bots to move command-and-control servers to other countries where enforcement is weaker.[1]

We find limited evidence that domestic enforcement deters attacks originating from the respective country. However, we find compelling evidence of a displacement effect: U.S. enforcement substantially *increases* attacks originating from *other countries*. Our findings are statistically consistent and efficient, and are robust to enforcement at different severity levels and to the various assumptions about the effective time window of the enforcement.

2. Model and Methodology

In our empirical analysis, we will test a parsimonious model of information security attacks. This model derives from economic research into the causes of crime in general. Government enforcement plays the central deterrent role in the economic analysis of crime [4] [20]. Increased enforcement reduces the crime rate by deterring criminal activity [5] [17]. Punishment includes possibly fines, imprisonment, and community service. In the particular context of information security, enforcement has also been hypothesized to deter attacks [10] [13] [16] [19], and methods of punishment also include restrictions on computer access.

Another factor in economic analyses of crime is the unemployment rate [21]. Increases in unemployment are associated with fewer legitimate employment opportunities, and hence more crime. The same applies to the context of information security. The lack of employment opportunities results in lower perceived opportunity cost of conviction, which increases hackers'

• Department of Information Systems, National University of Singapore, 3 Science Drive 2, Singapore 117543. Corresponding author: Qiu-Hong Wang, Tel: +65 6516-2831. We gratefully acknowledge financial support from the Asian Office of Aerospace R&D, award FA4869-07-1-4046.

[1]Bots are programs that are covertly installed on a user's machine to allow unauthorized user to control the computer remotely. Command-and-control servers are computers that perpetrators of bots use to relay commands and instructions to the bot-infected computers (Symantec Internet Security Threat Report, 2007)

1530-1605/08 $25.00 © 2008 IEEE

perceived net benefits from attack [15]. For instance, the Internet Crime Complaint Center reported that, "Frustrated with the employment possibilities offered in Romania, some of the world's most talented computer students are exploiting their talents online".[2]

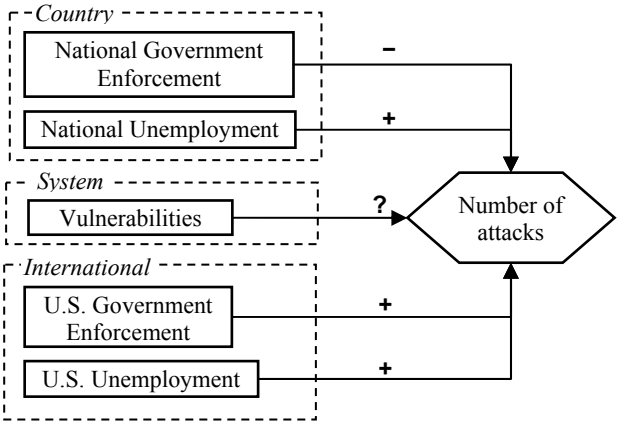

Figure 1. Information security attack model

The third factor in our parsimonious model is the opportunity for information security attacks. The existence of software/hardware vulnerabilities is one of the most important factors in the propensity for attacks against information security [3]. A "vulnerability" is a technical flaw or weakness in the design, implementation, or operation and management that can be exploited to violate the system's security policy.[3] The disclosure of vulnerabilities has two sided effects [14]. Timely reports about discovered vulnerabilities together with their fixing patches enable end-users to take precautions against potential information security attacks. However, these reports provide detailed technical descriptions of the vulnerabilities and their corresponding exploits (which are the ways to exploit the vulnerability), and so they might also facilitate attackers.

We also consider cross-country factors in information security. Information and communication technology has facilitated information security attacks across national boundaries. While conventional criminals tend to be localized, digital criminals can easily cross national boundaries and evade conviction by exploiting jurisdictional limitations between countries [15].[4] Having the most extensive technology infrastructure, the United States accounted for 31% of worldwide malicious activity (more than three times the share of second-ranked China) and was home to 40% of all known command-and-control servers in the world (four times the share of second-ranked South Korea). Thus, U.S. enforcement action may prompt perpetrators of bots to relocate their command-and-control servers to countries where enforcement is weaker.

Figure 1 summarizes our theoretical model. We speculate that national unemployment would have a positive effect on the number of attacks while the relationship between the number of published vulnerability notes and the number of attacks is ambiguous.

The event study methodology was developed by Fama, Fisher, Jensen, and Roll [12] to measure the impact of unanticipated changes in information on stock prices over a discrete time window, where the impact might possibly be temporary. Generally, the measured impact, which is called the "abnormal return", is the difference between the return on the stock with and without the unanticipated change in information. The return on the stock with the change in information is the actual return, while the return without the change is forecast from an empirical model (see, for instance, [18]).

In the context of information security, Campbell et. al. [8] directly applied the event study methodology to measure the impact of news reports of breaches of information security among publicly traded U.S. corporations.[5]

By contrast, our focus is the impact of enforcement on information security attacks rather than stock market reactions. The most obvious way to adapt the event study methodology is to construct an empirical model to predict the number of attacks absent enforcement, and then to measure the impact of enforcement by the difference between the actual and predicted number of attacks. However, as we explain in Section 5 below, this approach suffers serious shortcomings in the context of information security attacks.

Accordingly, we offer the following alternative adaptation of the event study. Apply linear regression with the number of attacks as the dependent variable and indicators of enforcement events as independent variables. To account for any cross-sectional heteroskedasticity and within-country serial correlation [6], we estimated standard errors using a robust covariance matrix. This procedure yields estimates of the coefficients which are consistent and efficient. The specific model is

$$\log A_{it} = \alpha + \beta \times \log V_t + \gamma_1 \times \log U_{it} + \gamma_2 \times P_{it} + \gamma_3 \times \log U_{Ut} + \gamma_4 \times P_{Ut} + \gamma_5 D_i \quad (1)$$

where A_{it} is the number of attacks originating from country i at date t. We detail the explanatory variables in Table 1.

[2] http://www.cbsnews.com/stories/2003/10/20/tech/main578965.shtml.

[3] "A Complete Guide to the Common Vulnerability Scoring System (CVSS)", http://www.first.org/cvss/cvss-guide.html.

[4] Symantec reported that "Although China had the most bot-infected computers worldwide, it had only the fourth highest number of known command-and-control servers worldwide …… This discrepancy likely indicates that the majority of bot-infected computers in China are being controlled from servers in other countries". (2007)

[5] Other applications of the event study methodology to study the stock-market impact of breaches of information security include [1] and [9].

Table 1. Explanatory variables

Explanatory variable	Definition
V_t	Cumulative number of vulnerabilities (since Jan. 1, 2003) subject to depreciation over time and differentiated as high, medium and low risk levels -- V_{ht}, V_{mt} and V_{lt} respectively.
U_{it}	National unemployment rate on a monthly basis
P_{it}	National enforcement event. P_{it}=1 if within the event window otherwise P_{it}=0.
U_{Ut}	U.S. unemployment rate on a monthly basis
P_{Ut}	U.S. enforcement event. P_t =1 if within the U.S. event window, otherwise P_t=0.
D_i	Country-specific dummy variables, which are used to control unobserved time-constant but country-specific effects.

The event day is that when government enforcement is first disclosed to the public. A key issue in event studies is to specify the "event window". The minimum event window is one day – the day on which the information is disclosed. Practically, the event window should be extended to take account of information leakage prior to the event day and delayed effects that occur after the event day. Since we are dealing with the transmission of information to attackers rather than smoothly functioning stock markets, we decided that, as a baseline, the event window would be 15 days, comprising 7 pre-event days, the event day, and 7 post-event days. The 7 pre-event days would capture any delay between enforcement action and announcement in public media. Formally, if T_0 represents the event day, then the event window is T_0-7 to T_0+7. In robustness checks, we study the sensitivity of our results to alternative definitions of the event window.

3. Data

The SANS Institute established the Internet Storm Center (ISC) in 2001 to assist Internet Service Providers and end-users to defend against malicious attacks through the Internet. The ISC follows the data collection, analysis, and warning system used in weather forecasting. It collects data from intrusion detection systems and firewalls associated with over 500,000 Internet Protocol (IP) addresses in over 50 countries. The ISC draws samples from many diverse locations to provide an accurate representation of Internet activity. This information is compiled in the DShield database.

The ISC statistics are subject to two limitations. One is that it counts only those attacks that meet a certain severity threshold. The more serious limitation is that the ISC's statistics can only identify the originating country of the attacking packets by IP address, even though the packets may come from bot-infected computers which are under the remote control of attackers located in other countries. We do account for this, in part, by incorporating U.S. unemployment rate and enforcement action as factors in our model of information security attacks.

The ISC provided country-level reports only from January 2004 onward.[6] We cut off our data collection on June 30, 2006. The sample period comprised 30 months or about 912 days. However, for unknown reasons, ISC did not report attacks for some periods. Thus, the actual number of observations was only about 550 per country. The sample comprised 15 countries, as listed in Table 2.

We define the event as any government enforcement action against violators of information security over the Internet. To identify the event of interest, we searched Factiva, a proprietary electronic database of newspapers. We used the settings: Source: All Sources; Company: All Companies; Subject: All Subjects; Industry: All Industries; Region: All Regions; Language: English, Chinese-Traditional, Chinese-Simplified, German, French, Italian, Japanese, Korean, Dutch, or Swedish, for every country for which the language is an official language; and the keywords: hack* and (convict* or sentenc* or prosecut*), and the same search terms in the other languages. In addition, we searched other newspapers and Google for any other reports of government enforcement with the keywords: hack* and (convict* or sentence* or prosecut*) and the name of each of the sample countries.[7]

Following Symantec's definition of internet security threats, we focused on enforcement actions against the following security breaches: malicious codes (virus, worms, Trojan horse, back door), spam, phishing, bots, denial of service, exploits of vulnerability, and security risks including adware, spyware, misleading applications, and other programs that users may not want on their system. We excluded enforcement actions against violation of piracy and offline digital crimes (e.g., sabotage of physical network structure, monitoring ATM users, credit card cloning).

A typical report was: "A 21-year-old Indiana member of a hacking gang was sentenced to 21 months in prison for breaking into Defense Department computers, federal law enforcement officials said" (CMP TechWeb, May 12, 2005). If the same episode of enforcement was reported by more than one source, we simply counted the first source, and ignored later reports.

[6] The country-level number of reports published by ISC is defined as the average number of packets reported from each IP in the respective country.

[7] Reports in each of the various languages were compiled by different coders. However, owing to resource limitations, the reports were not double-checked by multiple coders.

As jail sentences are possibly more punitive than fines and other forms of punishment, we distinguished reports by the extent of enforcement. Enforcement without imprisonment included cases investigated, arrested, prosecuted, and convicted (with fine or community service but not jail), while the other category was enforcement with imprisonment.[8] However, the accuracy of the classification is subject to the information reported. For instance, an item of enforcement news from Japan on May 18, 2005 mentioned only "arrested". It was not always possible to effectively distinguish between the various forms of punishment. Table 2 summarizes the number of events by country.

We collected monthly unemployment rates from the European Union and OECD,[9] and the National Statistical Bureau of Taiwan. It might be conjectured that information security attacks depend more closely on unemployment among information technology professionals. The U.S. Department of Labor does report the unemployment rate in the information industry. However, such data is not available for most of the other countries in our sample. Accordingly, we had to use the overall unemployment rate.

We collected vulnerability data from the National Vulnerability Database (NVD). The NVD, sponsored by DHS National Cyber Security Division/US-CERT, is the U.S. government's repository of standards based vulnerability management data. It provides comprehensive information on disclosed vulnerabilities including their published date, severity, vulnerability type, and related exploit range, etc. Following the NVD, we categorized vulnerabilities according to their severity defined by CVSS score:[10] (i) High (CVSS 7-10); (ii) Medium (CVSS 4-6); (iii) Low (CVSS 0-3). We compiled the total number of each category of published vulnerability on a daily basis. The vulnerability variables vary over time but do not vary across countries.

As vulnerabilities published at earlier dates are more likely to have been fixed, we hypothesized that the opportunities for attacks would depend on the *depreciated* stock of vulnerabilities to date. Specifically, with January 1, 2003 as the baseline and T as the number of calendar days between January 1, 2003 and date t, the depreciated stock of high vulnerabilities would be

$$V_{ht} = \frac{1}{T}\sum_{k=1}^{T} v_{hk} \times k \qquad (2)$$

where v_{ht} is the total number of high-risk vulnerabilities published at date k. The definitions of V_{mt} and V_{lt} were similar. The formula (2) gives higher weight to more recently published vulnerabilities.

Table 3 provides summary statistics of the variables.

4. Empirical Results

Referring to Figure 1 and (1), as a baseline, we regressed the number of daily attacks in the 15 countries on the explanatory variables other than U.S. unemployment and enforcement during the period January.2004 to June.2006. The event window was 7 days before and after the event day. Using ordinary least squares (OLS) without any adjustment for standard errors, the panel data exhibited high serial correlation (F test=78.85) and significant heteroskedasticity (χ^2 = 3937.29). Hence, we employed the robust covariance matrix estimator (a generalized White formula) which has been widely used in panel data studies to adjust for within-panel serial correlation [6] [11].

The results are reported in Table 4, column (a). All the estimated coefficients had the expected signs. Among them, the coefficient of national unemployment rate was positive but insignificant. The coefficient of enforcement was negative but insignificant. As predicted, the high- and low- risk vulnerabilities had significantly positive effects on the number of attacks. However, the effect of the medium-risk vulnerabilities was insignificant – possibly due to the much smaller number of such vulnerabilities as compared with the other two categories.

We next incorporated the U.S. unemployment rate and enforcement into the estimation, while excluding the U.S. observations from the sample. The results are reported in Table 4, column (b). All the estimated coefficients had the expected signs. Interestingly, U.S. enforcement was associated with a significantly positive effect on the number of attacks originating from other countries. On average, a U.S. enforcement action was associated with 15.49% (±1.57%) increase in the number of attacks originating from other countries. As U.S. factors accounted for part of the increase in the number of attacks, the deterrent effect of the national enforcement on the number of attacks increased in absolute value from 0.68% (±4.86%) in specification (a) to 1.89%(±4.97%) in speculation (b), but was still insignificant.

These estimation results provide evidence for the existence of a cross-boundary *displacement effect* of enforcement actions. Specifically, announcement of U.S. enforcement against internet security violators may persuade perpetrators to relocate their command-and-control servers or bot-infected networks to other countries where enforcement is weaker.

To check the robustness of our results, we re-estimated equation (1) with the event window changed from 7 days before and after the event day to only 7 days after the event day or 14 days after the event day. The

[8] The details about each event and the corresponding sources of the information are available from the authors upon request.

[9] http://ec.europa.eu; http://www.oecd.org respectively.

[10] CVSS is designed to rank information system vulnerabilities and provide the end user with a composite score representing the overall severity and risk the vulnerability presents.

estimation results are listed in Table 4, columns (c) and (d) respectively. The coefficients of all variables except had the expected signs with only slight change in magnitude. There was some evidence that both national and U.S. enforcement had effect before the publication of the information. Specifically, the deterrent effect of national enforcement was -1.89 %(±4.97%) with the event window of 7 days before and after the event day as compared to -1.11%(±4.20%) with the event window of 14 days after the event day. Similarly, the displacement effect of U.S. enforcement was 15.49 %(±1.57%) with the event window of 7 days before and after the event day as compared to 5.78%(±2.42%) with the event window of 14 days after the event day. These estimation results are consistent with the findings in specification (b) and further disclose the pre-event response in the timing of attacks and the heterogeneity in the composition of attacks originating from the respective countries.

We further distinguished enforcement into two categories: enforcement without imprisonment and enforcement with imprisonment. The results are reported in column (e) of Table 4. National enforcement with imprisonment had a relatively large but still insignificant deterrent effect on the number of attacks, while the impact from the national non-imprisonment enforcement was much smaller and even insignificantly positive. Both the U.S. non-imprisonment and imprisonment enforcement had significantly positive impact on attacks. Surprisingly, the impact of enforcement with imprisonment was smaller. This is counterintuitive since we expected a stronger displacement effect with more severe penalties.

Since the overall unemployment rate may not be a perfect proxy for the unemployment rate in information industry, we replaced the U.S. overall unemployment rate with its unemployment rate in the information industry. The results are reported in the last column of Table 4. This change did not affect the estimated coefficients very much. The impact of the U.S. enforcement events became slightly bigger than that of specification (b). Interestingly, a 1% increase in the U.S. information industry unemployment rate was associated with 109.63% increase in the number of attacks originating from the other countries, which was double the impact of the U.S. overall unemployment rate reported in specification (b). This is consistent with the thinking that unemployed IT professionals are the main source of information security attacks.

Lastly, similar to Campbell, et. al. [8], we used the seemingly unrelated regressions model to examine whether the national and U.S. enforcement affected the 14 other countries in a similar manner. Using a Wald Test, we rejected the null hypothesis that the coefficients of national enforcement were equal across countries at the 99.5% level (χ^2 = 30.79). However, we could not reject the null hypothesis that the coefficient of U.S. enforcement was the same across countries (χ^2 = 3.61). Our findings were also robust to estimation by Feasible General Least Squares (FGLS) with heteroskedastic and panel-specific autocorrelation error structure.

5. Alternative methodology

As mentioned above, the impact of enforcement actions on information security attacks could be measured by directly adapting the event study methodology from finance and economics [18]. This approach would construct an empirical model to predict the number of attacks absent enforcement, and then measure the impact of enforcement by the difference between the actual and predicted number of attacks. Specifically, for an event on date T_0, the test statistic would be based on the cumulative discrepancy in the number of attacks over the event window divided by its variance.

This approach is subject to two serious shortcomings. One is the assumption of uncontaminated estimation period [2]. Several of the enforcement events listed in Table 1 occurred close in time, resulting in an overlap between the estimation period of one event and the event windows of other events.

Second, our study used cross-country time series data, and as mentioned above, was subject to cross-country heteroskedasticity and serial correlation within countries.

Anyhow, we did apply this direct adaptation. To build the predictive model, we had to reserve part of the data for the "estimation window". This reduced the number of events that could be studied, and the sample countries to 9.[11]

Using the adapted "market model", the estimates showed that, in the United States, Great Britain, Italy and Sweden, reports of government enforcement were associated with an average 12% reduction in the number of attacks against computer networks within a 15-day window. This effect was statistically and economically significant. These 4 countries accounted for more than 68% of the enforcement actions and 86% of sentences of imprisonment among the 9 countries. However, for the other 5 countries, the effect of enforcement was ambiguous.

6. Concluding Remarks

We have made two main contributions. First, we presented two methodologies to adapt the event study from research in finance and economics to another context where high-frequency data on the variable of interest is available. The preferred methodology uses

[11] Australia, Brazil, Spain, Netherlands, Poland and Taiwan (China) were excluded due to the absence of events or insufficient observations within the event window.

linear regression with the number of attacks as the dependent variable and indicators of enforcement events as independent variables.

Our second contribution was the empirical finding that U.S. enforcement and unemployment had a substantial displacement effect. Increases in U.S. enforcement and unemployment were associated with substantial increases in information security attacks arising from other countries. The implication is that, in a networked world, national enforcement is not sufficient to deter cybercrimes. International cooperation in enforcement is essential.

References

[1]. Acquisti, A., Friedman, A., and Telang, R. "Is There a Cost to Privacy Breaches? An Event Study", 5th Workshop on the Economics of Information Security (WEIS), Cambridge, UK, 2006.

[2]. Aktas, Nihat, Eric de Bodt and Jean-Gabriel Cousin," Event studies with a contaminated estimation period", Journal of Corporate Finance, Volume 13, Issue 1, March 2007, 129-145.

[3]. Arora, Ashish, Anand Nandkumar and Rahul Teland, "Does information security attack frequency increase with vulnerability disclosure? An empirical analysis", Information Systems Frontier, Vol.8, Issue 5, 350-362.

[4]. Becker, Gary, "Crime and Punishment: An Economic Approach", Journal of Political Economy, Vol. 76 No. 2, March-April 1968, 169-217.

[5]. Benson, Bruce L., Iljoong Kim, and David W. Rasmussen, "Estimating Deterrence Effects: A Public Choice Perspective on the Economics of Crime Literature", Southern Economic Journal, Vol. 61, 1994.

[6]. Bertrand, Marianne, Esther Duflo, and Sendhil Mullainathan, "How Much Should We Trust Differences-In-Differences Estimations?" Quarterly Journal of Economics, Vol. 119 No. 1, February 2004, 249-275.

[7]. Cameron, Samuel, "The Economics of Crime Deterrence: A Survey of Theory and Evidence", Kyklos, Vol. 41 No. 2, May 1988, 301-323.

[8]. Campbell, K., L. A. Gordon, M. P. Loeb and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," Journal of Computer Security, Vol. 11, 2003, 431-448.

[9]. Cavusoglu, H., Mishra, B., and Raghunathan, S. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers", Working Paper, University of Texas, Dallas, 2002.

[10]. Choi, Jay Pil, Chaim Fershtman, and Neil Gandal, "Internet Security, Vulnerability Disclosure, and Software Provision", Working Paper, Michigan State University, July 2006.

[11]. Donald, Stephen G., and Kevin Lang, "Inference with Difference-in-Differences and Other Panel Data", Review of Economics and Statistics, Vol. 89 No. 2, May 2007, 221-233.

[12]. Fama, E. F., L. Fisher, M. C. Jensen, and R. Roll, "The Adjustment of Stock Prices to New Information", International Economic Review, Vol.10, No.1, 1969, 1-21.

[13]. Heal, Geoffrey, and Howard Kunreuther, "Interdependent Security: A General Model", Working Paper 10706, National Bureau of Economic Research, August 2004.

[14]. Kannan, Karthik and Rahul Telang, "Market for Software Vulnerabilities? Think Again", Management Science, Vol. 51, No. 5, May 2005, 726–740.

[15]. Kshetri, Nir, "The Simple Economics of Cybercrimes", IEEE Security & Privacy, January/February 2006, 33-39.

[16]. Kunreuther, Howard, and Geoffrey Heal. "Interdependent Security", Journal of Risk and Uncertainty, Vol. 26, Nos. 2-3, March 2003, 231-249.

[17]. Levitt, Steven D, "Using Electoral Cycles in Police Hiring to Estimate the Effect of Police on Crime," American Economic Review, Vol. 87 No. 3, June 1997, 270-290.

[18]. Mackinlay, A. R. "Event Studies in Economics and Finance", Journal of Economic Literature, Vol. 35 No. 1, March 1997, 13-39.

[19]. Png, I. P. L., Tang, C. Q., and Wang, Q. H. "Hackers, Users, Information Security: Welfare Analysis", 5th Workshop on the Economics of Information Security (WEIS), Cambridge, UK, 2006.

[20]. Polinsky, A. Mitchell, and Steven Shavell, "The Economic Theory of Public Enforcement of Law", Journal of Economic Literature, Vol. 38, March 2000, 45-77.

[21]. Raphael, Steven, and Rudolf Winter-Ebmer, "Identifying the Effect of Unemployment on Crime", Journal of Law and Economics, Vol. 44 No. 1, 2001, 259-284.

Table 2. Sample countries and event dates

Country	No. of sample days	No. of events	The earliest dates of reports of enforcement action (year-month-day) (by penalty)*	
AU (Australia)	570	5	Prosecuted	20050914
			Convicted	20060214
			Convicted with Jail	20041014; 20050915; 20050917
BR (Brazil)	565	3	Probed	20040917
			Arrested	20050826
			Convicted with Jail	20040105
CA (Canada)	558	5	Arrested	20040528
			Prosecuted	20051117
			Convicted with Jail	20050106; 20060117; 20060125
DE (Germany)	550	10	Probed	20041216; 20060511
			Arrested	20040317; 20060404
			Convicted	20060601
			Convicted with Jail	20040509; 20040514; 20040909; 20050706; 20050709
ES (Spain)	548	2	Convicted with Jail	20060213; 20060408
FR (France)	548	12	Probed	20040526
			Arrested	20040605; 20041021; 20041223; 20050510; 20060616
			Prosecuted	20040513; 20060513
			Convicted	20040601; 20060331; 20060408
			Convicted with Jail	20060602
GB (Great Britain)	546	14	Arrested	20040202; 20050128; 20050130
			Prosecuted	20040707; 20051105
			Convicted	20040209; 20040916; 20051007
			Convicted with Jail	20040203; 20040623; 20051008; 20051230; 20060117; 20060510
IT (Italy)	545	25	Probed	20040618; 20040828; 20050428; 20050919
			Arrested	20040410; 20050117; 20050128; 20060101; 20060206
			Prosecuted	20040312; 20040511; 20040917; 20041215; 20050105; 20050215; 20050531; 20050618; 20050716; 20050722; 20050825; 20050903; 20060211; 20060213; 20060422;

				20060608; 20060702
			Convicted with Jail	20060331
JP (Japan)	546	6	Probed	20050414
			Arrested	20050518; 20051110; 20051129
			Convicted with Jail	20041119; 20050325
KR (Korea)	545	23	Probed	20040620; 20040705; 20040715; 20040720; 20040729; 20041007; 20041021; 20041224; 20050604; 20050928; 20051213
			Arrested	20040413; 20041012; 20041013; 20050706; 20050709; 20050712; 20060517; 20060521
			Prosecuted	20041112; 20041123
			Convicted	20051016
			Convicted with Jail	20050929
NL (Netherlands)	545	0	N.A.	
PL (Poland)	545	0	N.A.	
SE (Sweden)	544	8	Probed	0060302; 20060605
			Arrested	20050317; 20050511; 20050609
			Convicted with Jail	20050309; 20050401; 20050914
TW (Taiwan, China)	544	1	Convicted with Jail	20040528
US (United States)	546	73	Probed	20060322; 20060515
			Prosecuted	20040301; 20040717; 20040817; 20050827
			Convicted	20040623; 20040625; 20050225; 20050609; 20050802; 20060616
			Convicted with Jail	20040109; 20040223; 20040305; 20040326; 20040528; 20040713; 20040719; 20040720; 20040805; 20040812; 20040824; 20040907; 20041019; 20041110; 20041215; 20041216; 20041217; 20041218; 20041223; 20041231; 20050112; 20050129; 20050203; 20050212; 20050314; 20050315; 20050315; 20050415; 20050415; 20050505; 20050512; 20050610; 20050611; 20050624; 20050816; 20050907; 20050909; 20050914; 20051014; 20051022; 20051202; 20051229; 20060124; 20060128; 20060213; 20060301; 20060322; 20060413; 20060421; 20060504; 20060506; 20060507; 20060509; 20060510; 20060511; 20060516; 20060525; 20060608; 20060609; 20060623; 20060626

*the events may not occur at the sample date

Table 3. Descriptive statistics (15 countries)

		Source	Total No. of sample days	Minimum	Maximum	Mean	Std. Deviation
Attacks		Internet Storm Center	8245	1706	23200000	1298673	2358852
Unemployment		OECD, Eurostat, etc.	8245	3.20	19.80	7.27	3.59
Vulnerability reports (by severity from low, medium to high)							
Daily number	High	National Vulnerability Database	8245	0	139	4.25	9.87
	Medium		8245	0	5	0.042	0.325
	Low		8245	0	13	0.269	0.906
Cumulative stock (since Jan 1, 2003)	High		8245	547	4497	2389.53	1308.80
	Medium		8245	132	158	151.03	5.97
	Low		8245	428	679	609.26	79.49
Cumulative stock with depreciation (since Jan 1, 2003)	High		8245	331.36	2968.68	1561.21	886.65
	Medium		8245	36.57	89.09	52.93	17.20
	Low		8245	212.11	303.78	254.65	26.10

Enforcement news (by penalty)

		Period	Total No. of events	Average No. of events across countries	Std. Deviation across countries
Probed	Factiva, Google, etc.	Jan 1, 2004 to June 30, 2006	24	1.60	2.75
Arrested			30	2.00	2.34
Prosecuted			29	1.93	4.19
Convicted			96	6.40	16.37
Convicted_with_Jail			92	6.13	14.77
Total			271	18.07	31.98

Table 4. OLS with robust variance matrix estimator

	a	b	c	d	e	f
Time window (T_0: the event day)	T_0-7~T_0+7	T_0-7~T_0+7	T_0+7	T_0+14	T_0-7~T_0+7	T_0-7~T_0+7
National enforcement	-0.0067955 (0.0474414)	-0.0191254 (0.0485502)	0.0048435 (0.0486785)	-0.0150528 (0.0589424)	--	-0.0190989 (0.048375)
National enforcement without imprisonment	--	--	--	--	0.0080233 (0.0420189)	--
National enforcement with imprisonment	--	--	--	--	-0.0774637 (0.0842701)	--
U.S. enforcement	--	0.1439844 (0.0156028)*** *	0.0766085 (0.0158947)*** *	0.0561961 (0.023903)**	--	0.1580682 (0.0197749)****
U.S. enforcement without	--	--	--	--	0.1934023 (0.0221521)****	--

imprisonment						
U.S. enforcement with imprisonment	--	--	--	--	0.0854386 (0.0135636)****	--
National unemp. rate	0.170061 (0.6857701)	0.0507902 (0.6879444)	0.0874796 (0.6999422)	0.0853231 (0.6918727)	0.1154549 (0.7053654)	0.0484437 (0.6883089)
U.S. unemp. rate	--	2.409503 (0.7003874)***	2.698826 (0.6902055)***	2.801747 (0.66789)****	2.430997 (0.7075884)***	--
U.S. information industry unemp. rate	--	--	--	--	--	4.015608 (1.177954)***
High vulnerability	1.159887 (0.16179)****	1.139581 (0.1595331)****	1.232965 (0.1563772)****	1.263089 (0.1500848)****	1.132351 (0.1557937)****	1.145853 (0.1607058)****
Medium vulnerability	1.806628 (.4139699)	1.395483 (.3552396)	1.55622 (.3411036)	1.636591 (.3481393)	1.26146 (.3362101)	1.426548 (.3531964)
Low vulnerability	3.788873 (0.7816227)****	3.341782 (0.7477701)****	3.250383 (0.7468017)****	3.161166 (0.7538922)****	3.597313 (0.7496893)****	3.267653 (0.7292944)****
Constant	-23.48926 (5.148146)****	-23.11254 (5.683123)****	-24.36316 (5.649486)****	-24.56666 (5.548753)****	-24.05831 (5.663607)****	-20.89587 (5.320344)***
# of Observations	8245	7699	7699	7699	7699	7699
Adj. R-Square	0.6795	0.4863	0.4825	0.4815	0.4888	0.4865
Impact of national enforcement	-0.68% (±4.86%)	-1.89% (±4.97%)	0.49% (±4.99%)	-1.11% (±4.20%)	0.81%(±4.29%)[1] -7.45%(±8.79%)[2]	-1.89% (±4.96%)
Impact of U.S. enforcement	--	15.49% (±1.57%).	7.96% (±1.60%)	5.78% (±2.42%)	21.34%(±2.24%)[3] 8.92%(±1.37%)[4]	17.12% (±2.00%)

**** significant at 99.9%; *** significant at 99%; ** significant at 95%; * significant at 90%.

Note:

1. The impact of national enforcement without imprisonment
2. The impact of national enforcement with imprisonment
3. The impact of U.S. enforcement without imprisonment
4. The impact of U.S. enforcement with imprisonment