The Deterrent Effect of Enforcement Against Computer Hackers:

Cross-Country Evidence

I.P.L. Png and Chen-yu Wang*

March 2007

* Department of Information Systems, National University of Singapore. Corresponding author: Ivan Png, tel: +65 6516-6807; http://www.comp.nus.edu.sg/~ipng/.

1. Introduction

That government enforcement effectively deters criminal behavior is the central premise in analyses of crime in general (Becker 1968; Stigler 1970; Polinsky and Shavell 2000) and information security in particular (Kunreuther and Heal 2003; Heal and Kunreuther 2004; Choi et al. 2006; Png et al. 2006). Early studies of the impact of enforcement on crime yielded inconclusive results (Cameron 1988). Only relatively recently have empirical studies shown that increased enforcement does indeed reduce crime (Benson et al. 1994; Levitt 1997).

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 8 countries over the period January 2004 to August 2006. Our empirical strategy adapts the event study methodology which has been widely used in the disciplines of finance and economics. From a newspaper database, we identified 49 reports of enforcement action in 8 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.

We find that reports of government enforcement are associated with an average 36% reduction in the number of attacks against computer networks during a 15-day window. This effect is statistically and economically significant.

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 (Becker 1968; Stigler 1970; Polinsky and Shavell 2000). Increased enforcement reduces the crime rate by deterring criminal activity (Benson et al. 1994;

Levitt 1997). Punishment includes possibly fines, imprisonment, and community service. In the particular context of information security, enforcement has also been hypothesized to deter attacks (Kunreuther and Heal 2003; Heal and Kunreuther 2004; Choi et al. 2006; Png et al. 2006), and methods of punishment also include restrictions on computer access.

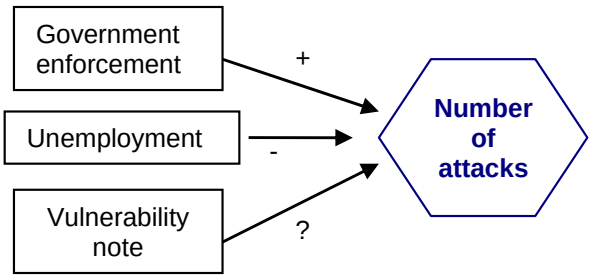
Another key factor in economic analyses of crime is the unemployment rate (Raphael and Winter-Ebmer 2001). The crime rate increases with the unemployment rate as more people participate in crime and people have more time to participate. The same applies to the context of information security. The lack of employment opportunities results in lower perceived monetary opportunity cost of conviction, which increases hackers' perceived net benefits from attack (Kshetri 2006). The U.S.-based Internet Crime Complaint Center, a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) reported that, "Frustrated with the employment possibilities offered in Romania, some of the world's most talented computer students are exploiting their talents online".[1]

The third factor in our parsimonious model is the opportunity for information security attacks. 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. The Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie-Mellon University and commercial security specialists systematically publish notes on new vulnerabilities in computer software and systems. They publish these notes in order to foster information security. However, these notes 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.

Figure 1 summarizes our theoretical model.

Figure 1: Influences on the number of attacks

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



The event study methodology was developed by Fama, Fisher, Jensen, and Roll (1969) 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 a statistical model (see, for instance, Mackinlay, 1997).

One implementation of the event study methodology uses the "market model", which represents the expected return on a stock, *i*, as

$$R_{it} = \hat{\alpha}_i + \hat{\beta}_i R_{mt} + \varepsilon_{it}, \qquad (1)$$

where R_{it} and R_{mt} are the expected returns on stock *i* and the entire market in period *t*, ε_{it} is the error in the model of the return, and which has zero expectation, $E(\varepsilon_{it}) = 0$, and variance σ_{ε_i}, and $\hat{\alpha}_i$ and $\hat{\beta}_i$ are estimated coefficients. The abnormal return on the stock is then

$$\varepsilon_{it} = R_{it} - \hat{\alpha}_i - \hat{\beta}_i R_{mt}. \qquad (2)$$

Any abnormal return arising from an event can be discovered by testing the null hypothesis that the cross-sectional mean of ε_{it} is zero. Any significant difference

from zero implies that some portion of the observed return cannot be accounted for by market fluctuations and indeed captures the impact of the specific event.2

Referring to Figure 4.1, we adapt the market model to information security attacks by supposing that the number of attacks in country *i* in day *t* in the absence of government enforcement is

$$E(ATK_{it}) = \hat{\beta}_i + \hat{\alpha}_{1i} UR_{it} + \hat{\alpha}_2 VDOS_t + \hat{\alpha}_3 VBUF_t + \hat{\alpha}_4 VOTH_t, \qquad (3)$$

where UR_{it} is the corresponding unemployment rate on a monthly basis, $VDOS_t$ is the number of vulnerability notes relating to Denial of Service attacks published that day, $VBUF_t$ is the number of vulnerability notes relating to Buffer Overflow published that day, and $VOTH_t$ is the number of other vulnerability notes published that day.[3]

In our adaptation, the events are reports of government enforcement against information security attackers. The discrepancy in the number of attacks is the difference between the actual number of attacks and the predicted number of attacks, as predicted by the model (3):[4]

$$\begin{aligned} \Delta ATK_{it} &= ATK_{it} - E(ATK_{it}) \\ &= ATK_{it} - \hat{\beta}_i - \hat{\alpha}_{1i} UR_{it} - \hat{\alpha}_2 VDOS_t - \hat{\alpha}_3 VBUF_t - \hat{\alpha}_4 VOTH_t. \end{aligned} \qquad (4)$$

We next explain in detail the procedure and statistical inference:

Step 1: 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, which is the unit of analysis in time. The smallest event window is one day – the day on which the information is disclosed. Practically, the event window is extended to take account

[2] The event study methodology has been directly applied in the context of information security to measure the impact of vulnerability disclosures on vendors' stock prices (Telang and Wattal 2005) and announcements of breaches of information security (Cavusoglu et al 2002; Acquisti, Friedman, and Telang 2006).
[3] We explain these variables in detail in the following section on Data.
[4] In the event study methodology, this is called the "abnormal return".

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 the event window would be 15 days, comprising 7 pre-event days, the event day, and 7 post-event days. If the event day is represented by T_0, the event window is then $T_0 - 7$ to $T_0 + 7$.

Step 2: The next issue is the period over which to estimate the model of the expected number of attacks absent government enforcement, (3). The longer is the estimation period, the more accurately can the coefficients can be estimated. However, a longer estimation period would reduce the number of events that can be studied. Since our data is limited to the 32-month period, January 2004 to August 2006, and unemployment is seasonal, we chose the estimation period to be a 12-month period, January to December 2004. However, owing to some gap in the ISC's records, data on attacks were available for only 68 days during January to December 2004. So, the estimation period actually comprised 68 days, hence the estimation period for each event was from $T_0 - 75$ to $T_0 - 8$.

Step 3: We used ordinary least squares (OLS) to estimate the coefficients of the model, (3).

Step 4: For an event on some date T_0, the test statistic is based on the cumulative discrepancy in the number of attacks over the event window,

$$CDA_i(T_0 - 7, T_0 + 7) = \sum_{t=T_0-7}^{T_0+7} \Delta ATK_{it} \,. \qquad (5)$$

As the estimation period increases in length, the asymptotic variance of CDA_i is

$$\begin{aligned} \sigma_i^{\,2}(T_0 - 7, T_0 + 7) &= ((T_0 + 7) - (T_0 - 7) + 1)\sigma_{\varepsilon_i}^{\,2} = 15\sigma_{\varepsilon_i}^{\,2} \\ &= 15/(68 - 5) \cdot \sum_{t=T_0-75}^{T_0-8} (R_t - \hat{\beta} - \hat{\alpha}_1 UR_t - \hat{\alpha}_2 VD_t - \hat{\alpha}_3 VB_t - \hat{\alpha}_4 VO_t)^2 . \end{aligned} \qquad (6)$$

Hence the cumulative discrepancy in the number of attacks has an asymptotic normal

distribution with the variance as stated in (6).

With *M* events, the average cumulative discrepancy is

$$\overline{CDA}(T_0 - 7, T_0 + 7) = \frac{1}{M}\sum_{i=1}^{M} CDA_i(T_0 - 7, T_0 + 7), \quad (7)$$

which has an asymptotic normal distribution with variance,

$$\text{var}(\overline{CDA}(T_0 - 7, T_0 + 7)) = \frac{1}{M^2}\sum_{i=1}^{M} \sigma_i^{\,2}(T_0 - 7, T_0 + 7). \quad (8)$$

Step 5: The final step is to test the null hypothesis using the statistic,

$$\theta = \frac{\overline{CAR}(T_0 - 7, T_0 + 7)}{\text{var}(\overline{CAR}(T_0 - 7, T_0 + 7)^{1/2}}. \quad (9)$$

By (7) and (8), this statistic has an asymptotic normal distribution with zero mean and unit variance.

3. Methodology and Data

The SANS Institute established the Internet Storm Center (ISC) (http://isc.sans.org/) 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 addresses in over 50 countries. The ISC draws samples from many diverse locations to provide an accurate representation of current Internet activity. This information is compiled in the DShield database.

The statistics published by the ISC 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 only include the top 20 countries by number of attacks, and the top 20 change daily. This presents us with a difficult trade-off: if we

include more countries in the study, we can get a broader view of the impact of enforcement. However, the more countries are included, the lower will be the likelihood of the data on attacks being available for all of the countries on each of the sampling days.

The ISC provided country-level reports only from January 2004 onward. We cut off our data collection on August 1, 2006. The sample period comprises 31 months or about 940 days. However, since the ISC reports only data for the top 20 countries, the actual number of observations is only about 600 per country. Further, we need data for all of the sample countries on the same day. We decided to limit the data collection to countries for which we could procure data on attacks for every one of at least 300 days. The sample comprised 16 countries, as listed in Table 1.

The first sample day was 2004/1/5, followed by 2004/1/7, 2004/1/11, 2004/1/23, …, and ending with , 2006/6/20, 2006/6/22, and 2006/7/26. Note that the intervals between consecutive sample days were not uniform. In the spirit of event study methodology, in which time is measured by trading days, we measured estimation periods and event windows by sampling days rather than calendar days.

To identify the event of interest – government enforcement, 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 or Chinese-Traditional or Chinese-Simplified, and the keywords: hack* and (convict* or sentenc* or prosecut*). 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.

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, 12 May 2005). If the same episode of enforcement was reported by more than one source, we simply counted the first source, and ignored later reports.

As jail sentences are possibly more painful than fines and other forms of

punishment, we distinguished reports of jail (EJAIL) from reports of other forms of punishment (ENOTJAIL). The Appendix lists the events and the corresponding sources of the information. However, as the detailed list shows, e.g., China, 11 July 2005, "Arrested", it is difficult to make an effective distinction between the various forms of punishment. Hence, in the estimates, we combined EJAIL and ENONJAIL into a single series of events. Table 1 summarizes the number of events by country.

We collected monthly unemployment rates from various sources, including Eurostat (http://ec.europa.eu/index_en.htm), OECD (http://www.oecd.org/home/), the Korean National Statistical Office, the National Statistical Bureau of Taiwan, and China Monthly Economic Indicators.

Vulnerability notes encompass various security attacks and compute-related exploits. Based on Fadia's (2006) classification and the vulnerability notes published by CERT/CC and SecurityFocus, we categorized vulnerability notes into three groups: (i) Denial of Service and Distributed Denial of Service (VDOS), (ii) security breaches relating to Buffer Overflow (VBUFFER), and (iii) other security breaches, such as IP Spoofing Attacks, Windows Attacks, and Input Validation Vulnerabilities (VOTHERS).

We collected the vulnerability notes from CERT/CC (http://www.cert.org) and SecurityFocus (http://www.securityfocus.com). CERT/CC's Vulnerability Notes Database lists vulnerabilities with descriptions, impact, as well as solutions. SecurityFocus lists vulnerabilities with information, discussion, exploit, solution, and references. For each day, the value of each vulnerability variable is the sum of the numbers of notes published by CERT/CC and SecurityFocus. The vulnerability variables vary over time but do not vary across countries.

Table 2 provides summary statistics of the variables. Table 3 provides the correlations among the variables. VBUF seems to be correlated with VDOS and VOTH. Otherwise, the explanatory variables appear to be uncorrelated.

4. Empirical Results

Recall from (7) that our test statistic is the average cumulative discrepancy, which is

the average of the difference between the observed number of attacks and the predicted number of attacks (in the absence of any enforcement) over all the reported enforcement within the country during the sample period. For simplicity, the average cumulative discrepancy can be re-labeled as the "average deterrent effect".

Table 4, column (d), reports our results on the average deterrent effect. The results are quite sharp. In all 8 countries, reports of enforcement have a significant negative effect on the number of attacks. In absolute terms, the impact varies from -1.13*106 in the Netherlands to -1.60*107 in Spain.

To place these numbers in perspective, we also measured the deterrent effect relative to the average daily number of attacks. We normalize the average deterrent effect by the number of sample days. For instance, in the case of Canada, we identified three events with 10, 11, and 11 sample days, respectively. The average number of sampling days was [10 + 11 + 11] ÷ 3 = 11. We then divided the normalized deterrent effect by the average daily number of attacks to obtain the relative deterrent effect.

Table 4, column (e), reports the results for the relative deterrent effect. The magnitude of the effect varies dramatically with the largest being 84.66% (Spain) and the smallest being 10.12% (U.S.). The relative deterrent effects of most countries fall within the range from 19% to 43%, with the average being 35.64%. Apparently, reports of enforcement have an economically significant deterrent effect on computer attacks. Specifically, such reports are associated with a 36% reduction in the number of attacks during the 15-day event window.

To check the robustness of the preceding estimates and also to investigate whether the effect of enforcement decays over time, we next repeated the estimates using a longer event window of 22 days, comprising 7 pre-event days, the event day, and 14 post-event days.[5] Table 4, column (f), presents the results with the 22-day event windows. For all 8 countries, the deterrent effect is statistically significant. In the cases of Canada, China, Great Britain, Korea, and the United States, the effect of enforcement decays substantially. By contrast, for Spain and Netherlands, the effect

[5] The conventional approach in event studies is to use symmetric event windows. We use an asymmetric event window as we aim to measure the impact of enforcement over time.

of enforcement appears to intensify over time. We have no good explanation for these differences.

5. Concluding Remarks

Our research has made two contributions. It has established that government enforcement reduces attacks against computer networks by an average of 36% during a 15-day window. This provides empirical justification for investment of public resources in enforcement action. It also lends support to analytical models of deterrence including those of Kunreuther and Heal (2003), Heal and Kunreuther (2004), Choi et al. (2006), and Png et al. (2006).

The other contribution is to demonstrate that the methodology of the event study from research in finance and accounting can be adapted to another context where high-frequency data on the variable of interest is available.

Our findings are subject to several limitations. First, the event study methodology focuses on a limited event window. The deterrent effect that we have detected may well be temporary. Hackers may be frightened, but over time, memories of the enforcement may fade, and they return to malicious activity. Indeed, for some countries, we noted some decay in the deterrent effect even within 15 days. Further work could focus on long-term vis-à-vis immediate deterrence.

Second, we could not effectively distinguish between reports of jail and other forms of punishment. Superficially at least, imprisonment should have greater deterrent effect than fines, community service, or restrictions on computer usage. Future work could aim to compare the deterrent effects of various forms of punishment.

Finally, for simplicity, we applied asymptotic distributions to compute the test statistic. However, the number of events varied from 1 to 17, with an average of 9.6. Accordingly, it might be more appropriate to apply small sample test statistics.

References

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.

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

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.

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

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.

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

Fadia, A., *Network Security - A Hacker's Perspective*, 2nd Edition, Thomson, Course Technology, 2006.

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.

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

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

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

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.

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

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.

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

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.

Stigler, George J., "The Optimum Enforcement of Laws", *Journal of Political Economy*, Vol. 78 No. 3, May-June 1970, 526-536.

Telang, Rahul, and Sunil Wattal, "Impact of Software Vulnerability Announcements on the Market Value of Software Vendors - An Empirical Investigation", 4th Workshop on the Economics of Information Security (WEIS), 2005.

Table 1: Sample Countries and Event Dates

Country	No. of sample days	No. of events	Dates of reports of enforcement action (year-month-day)
AU (Australia)	559	0	n.a.
BR (Brazil)	558	1	n.a.
CA (Canada)	572	3	2005.01.06; 2005.11.17; 2006.01.17
CN (China)	570	15	2005.03.21; 2005.03.23; 2005.07.11; 2005.07.12; 2005.10.19; 2005.11.08; 2005.11.14; 2005.11.15; 2005.11.18; 2006.02.24; 2006.04.10; 2006.04.15; 2006.04.22; 2006.04.27; 2006.05.12
DE (Germany)	562	1	n.a.
ES (Spain)	561	2	2006.02.07; 2006.04.08
FR (France)	561	0	n.a.
GB (Great Britain)	559	8	2005.01.30; 2005.10.10; 2005.11.05; 2005.12.30; 2006.01.17; 2006.05.10
IT (Italy)	519	0	n.a.
JP (Japan)	558	3	2005.03.25; 2005.04.14; 2005.11.10
KR (Korea)	559	2	2005.7.12; 2006.05.21
NL (Netherlands)	528	1	2005.10.10
PL (Poland)	516	0	n.a.
SE (Sweden)	413	0	n.a.
TW (Taiwan)	556	0	n.a.
US (United States)	559	25	2005.01.29; 2005.02.25; 2005.03.14; 2005.10.14; 2005.10.22; 2005.12.30; 2006.01.28; 2006.04.13; 2006.04.21; 2006.05.06; 2006.05.09; 2006.05.10; 2006.05.11; 2006.05.16; 2006.05.25; 2006.06.08; 2006.06.09.

Table 2: Descriptive Statistics

Variable	Source	Mean	Median	Max	Min	Std. Dev.
Number of attacks	Internet Storm Center	$1.45*10^{6}$	$6.19*10^{5}$	$1.74*10^{7}$	$2.35*10^{4}$	$2.34*10^{6}$
Unemp. rate	OECD, Eurostat, etc.	7.13%	6.10%	19.80%	3.20%	3.46%
EJAIL	Factiva	$8.54*10^{-3}$	0.00	1.00	0.00	$9.20*10^{-2}$
ENOTJAIL	Factiva	$5.83*10^{-3}$	0.00	1.00	0.00	$7.61*10^{-2}$
VDOS	CERT/CC, SecurityFocus	1.40	1.00	31.00	0.00	2.42
VBUF	CERT/CC, SecurityFocus	1.45	1.00	20.00	0.00	2.24
VOTH	CERT/CC, SecurityFocus	8.99	7.00	134.00	0.00	11.26

Table 3: Correlations

	Unemp. rate	EJAIL	ENOTJAIL	VDOS	VBUF	VOTH	No. of attacks
Unemp. rate	1						
EJAIL	-0.048**	1					
ENOTJAIL	-0.054**	0.260**	1				
VDOS	-0.011	0.025	0.011	1			
VBUF	-0.003	0.026	0.006	0.477**	1		
VOTH	-0.025	0.025	-0.004	0.0756**	0.587**	1	
No. of attacks	-0.177**	0.171**	0.122**	-0.022	-0.014	-0.034*	1

** Significant at the 0.01 level (2-tailed)

* Significant at the 0.05 level (2-tailed)

Table 4: Average Deterrent Effect

Country	(a) Average no. of attacks (daily)	(b) No. of events	(c) Average sample days	(d) Average Deterrent Effect (*p*-value)	(e) = (d)/(c) ÷ (a) Relative deterrent effect	(f) Average deterrent effect over 22-day window (*p*-value)
CA (Canada)	$1.03*10^6$	3	11	-2.20×10^6 (5.38×10^5)***	19.42%	-1.86×10^6 (6.13×10^5)**
CN (China)	$3.28*10^6$	15	11	-1.18×10^7 (1.05×10^6)***	32.71%	-4.66×10^6 (1.22×10^6)***
ES (Spain)	$1.89*10^6$	2	10	-1.60×10^7 (1.19×10^6)***	84.66%	-3.02×10^7 (1.46×10^6)***
GB (Great Britain)	$6.95*10^5$	6	10	-2.44×10^6 (2.43×10^5)***	35.11%	-2.03×10^6 (2.89×10^5)***
JP (Japan)	$7.27*10^5$	3	8	-1.36×10^6 (4.75×10^5)**	23.38%	-1.40×10^6 (5.47×10^5)**
NL (Netherlands)	$4.33*10^5$	1	7	-1.13×10^6 (4.25×10^5)**	37.28%	-3.01×10^6 (6.03×10^5)***
KR (South Korea)	$7.91*10^5$	2	10	-3.36×10^6 (5.75×10^5)***	42.48%	-9.89×10^5 (6.27×10^5)
US (United States)	$9.29*10^6$	17	10	-9.40×10^6 (1.47×10^6)***	10.12%	-5.54×10^6 (1.81×10^6)**
			77			

Appendix: Detailed list of reports

Country	Event Date	Event Description	Source
CA	2005.01.06	9 months probation	National Post
	2005.11.17	Suspended from school for 30 days and is facing an expulsion hearing	The Toronto Star
	2006.01.17	3 years and 9 months in jail	Birmingham Post
CN	2005.03.21	a token fine of 1 RMB	http://www.315safe.com
	2005.03.23	Sentenced to 3 to 4 years in prison and fines	China Youth Daily
	2005.07.11	Arrested	BBC Monitoring Asia Pacific
	2005.07.12	Sentenced to 3 years in prison and a fine of 12,000 RMB	Wenhui Daily
	2005.10.19	Arrested	South China Morning Post
	2005.11.08	Arrested and accused	South China Morning Post
	2005.11.14	Arrested	Xinhua News Agency
	2005.11.15	Conviction of theft	China Daily
	2005.11.18	a maximum sentence of 3 years	Shanghai Daily
	2006.02.24	Arrested	http://www.yesky.com
	2006.04.10	Not punished just warning	South China Morning Post
	2006.04.15	Arrested and being sentenced	Xinhua News Agency
	2006.04.22	Sentenced to 1 year in jail	Xinhua News Agency
	2006.04.27	Arrested	Xinhua News Agency
	2006.05.12	Sentenced to 4 to 6 months in jail	Shanghai Evening Post
ES	2006.02.07	2 years in jail	M2 Presswire
	2006.04.08	up to 40 years in jail	Agence France Presse
UK	2005.01.30		The Independent
	2005.10.10	Found guilty and fined £400	Leicester Mercury

	2005.11.05	Sent to jail	The Northern Echo
	2005.12.30	up to 10 years in jail	The Daily Telegraph
	2006.01.17	Jailed for 3 years and 9 months	Birmingham Post
	2006.05.10	Extradited to and convicted in the US, up to 50 years in jail	Press Association Newswire
JP	2005.03.25	an 8-month prison sentence, but suspended for 3 years	BBC Monitoring Asia Pacific
	2005.04.14	Being investigated	http://www.chinanews.com.cn
	2005.11.10	Arrested	Kyodo News
NL	2005.10.10	Arrested and convicted	Xinhua News Agency
KR	2005.7.12	Arrested	http://www.sunm.net
	2006.05.21	Arrested	http://www.ccidnet.com
US	2005.01.29	18 months in prison	The Commercial Appeal
	2005.02.25	Suspended sentence	Northern Territory News/Sunday Territorian
	2005.03.14	6 months in jail	MIS New Zealand
	2005.10.14	a maximum penalty of 5 years imprisonment and a $250,000 fine	Vancouver Sun
	2005.10.22	Sentenced to 7 months	Rocky Mountain News
	2005.12.30	up to 10 years in jail	The Daily Telegraph
	2006.01.28	2 years in prison	Calgary Herald
	2006.04.13	2 years' probation and 200 hours of community service	The Courier-Mail
	2006.04.21	up to 10 years in federal prison	http://www.silicon.com
	2006.05.06	1 year of probation and ordered to pay $7,427 in restitution	The News Tribune
	2006.05.09	10 years in prison	CMP TechWeb
	2006.05.10	5 years in federal prison	Associated Press Newswires

	2006.05.11	3 years of imprisonment	Ukrainian National News Agency
	2006.05.16	4 years and 9 months in jail	The Gold Coast Bulletin
	2006.05.25	Prison time	CMP TechWeb
	2006.06.08	up to 30 years in prison and reimbursed his former employer	The Independent
	2006.06.09	20 years in prison and a $250,000 fine	VNUNet United Kingdom