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

IVAN P.L. PNG, CHEN-YU WANG, AND QIU-HONG WANG

IVAN P.L. PNG is Lim Kim San Professor, Professor of Business Policy, and Professor of Information Systems and Economics at the National University of Singapore. His research focuses on the economics of intellectual property, information privacy, and pricing. Dr. Png is the author of *Managerial Economics,* which has been translated into Chinese (traditional and simplified characters) and Korean. He is a professorial fellow of the IP Academy of Singapore, and an associate editor of *Management Science.* He was a nominated Member of Parliament (10th Parliament of Singapore), 2005–6.

CHEN-YU WANG is a Foreign Exchange Trader at BNP Paribas, Singapore. He has an M.Sc. in Information Systems from the National University of Singapore.

QIU-HONG WANG is a Research Fellow at the Department of Business Policy, National University of Singapore. She received her Ph.D. in Information Systems from the National University of Singapore in 2007. Her research focuses on pricing, the economics of information security, the economics of intellectual property, and virtual economy.

ABSTRACT: We adapt the event study methodology from research in financial economics to study the impact of government enforcement and economic opportunities on information security attacks. We found limited evidence that domestic enforcement deters attacks within the country. However, we found compelling evidence of a displacement effect: U.S. enforcement substantially increases attacks originating from other countries. We also found strong evidence that attackers are economically motivated in that the number of attacks is increasing in the U.S. unemployment rate. Our findings were robust to differences in the effective time window of enforcement and the measurement of vulnerabilities.

KEY WORDS AND PHRASES: economics, information security, security attacks, security enforcement, unemployment rate.

THAT GOVERNMENT ENFORCEMENT EFFECTIVELY DETERS criminal behavior is the central premise in economic analyses of crime in general [4, 25], and information security in particular [8, 14, 19, 20, 24]. Empirical studies have shown that increased enforcement

Journal of Management Information Systems / Fall 2008, Vol. 25, No. 2, pp. 125–144.
© 2008 M.E. Sharpe, Inc.
0742–1222 / 2008 $9.50 + 0.00.
DOI 10.2753/MIS0742-1222250206

does indeed reduce crime [12]. However, information security is far removed from the crimes typically studied in the literature on the economics of enforcement—murder, assault, burglary, and so on. Accordingly, the empirical question of whether enforcement deters information security attackers remains an important open question.

A related issue is the motivation of information security attackers. Leading security vendor Symantec observed that the motivation of attackers has shifted toward making money. This trend portends greater losses as attackers aim “to create more malicious code and that will become stealthier and more selective” [28, p. 9]. The motivation of attackers is important for government policy and business strategy. Fines and other economic penalties will be more effective deterrents to the extent that attackers are motivated by economic gain.

In this paper, we investigate these issues using a sample of attacks on 15 countries over the January 2004–June 2006 period. Our empirical strategy adapts the event study methodology that has been widely used in the disciplines of finance and economics. We regress the number of attacks on indicators of enforcement events, unemployment rates, and other explanatory variables.

From a news database and other public news resources, we identified 192 reports of enforcement action against information security violators in the sample countries during the sample period. Using novel sources of data on information security attacks, we measured the impact of those enforcement actions and unemployment on the rate of information security attacks originating from the respective country. Since attack resources can be relocated and the United States is the largest source of information security attacks, we also investigated whether U.S. enforcement action and unemployment might *displace* attackers to other countries.

We found limited evidence that domestic enforcement deters attacks originating from the respective country, and little evidence that attacks increase with domestic unemployment. However, we found compelling evidence of a displacement effect: U.S. enforcement and unemployment substantially *increase* attacks originating from *other countries.* The results with respect to U.S. enforcement and unemployment verify that information security enforcement does have deterrent effects and that attackers are economically motivated.

Our findings were robust to alternative assumptions about the effective time window of the enforcement and the measurement of vulnerabilities.

Model and Methodology

In our empirical analysis, we test a parsimonious model of information security attacks. This model derives from economic analyses of crime in general, whereby potential criminals weigh the benefits and cost of crime [4, 12, 25]. In these analyses, the benefits may be pecuniary—the value of the items stolen—or nonpecuniary. The central premise is that government enforcement reduces crime either through deterrence or incapacitation.

In the context of information security, the trend is toward attacks for pecuniary gain, rather than to show off technical prowess or gain peer approval [15, 28]. Accordingly, the economic model of crime should apply to information security [8, 14, 19, 20, 24]. However, this remains to be empirically verified.

In our model, we characterize the attacker's benefit by the number of Internet users for the following reasons. Bots are programs that attackers covertly install to remotely control the machines of unsuspecting victims through command-and-control servers [29]. Attackers broadcast bots and viruses through the Internet. Hence, the attacker's benefit increases with the number of potential victims, which is essentially the Internet user population [24].[1]

With regard to the costs of crime, we consider two factors. One is government enforcement. Punishment possibly includes fines, community service, and imprisonment. Empirical studies have shown that increased enforcement is associated with lower crime [12]. Importantly, young offenders tend to behave myopically in responding to enforcement [21]. This is particularly germane to the context of information security as attackers require technical capability, and hence are likely to be relatively young. Accordingly, the impact of enforcement may be concentrated in the short term.

The other cost factor is alternative economic opportunities. Increases in unemployment are associated with fewer legitimate economic alternatives, and hence a lower opportunity cost of crime and more crime [12, 26]. The same applies in the context of information security [19]. Indeed, the Internet Fraud 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" [27].

The final element in our model relates to the feasibility of information security attacks. The existence of software and hardware vulnerabilities is one of the most important determinants of information security attacks [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 [23]. The disclosure of vulnerabilities has two conflicting effects [16]. Timely reports about vulnerabilities together with the relevant patches enable end users to take precautions against potential information security attacks. However, these reports provide detailed technical descriptions of the vulnerabilities, and so they might also facilitate the development of exploits (which are the technical ways to exploit the vulnerability), and so increase the number of attacks.

We also consider cross-country factors in information security. Information and communication technology has facilitated attacks across national boundaries. While conventional criminals tend to be localized, cyber criminals can easily cross national boundaries and exploit jurisdictional limitations between countries [19]. Having the most extensive technology infrastructure, the United States accounted for 31 percent of worldwide malicious activities (more than three times the share of second-ranked China) and was home to 40 percent of all known command-and-control servers in the world (four times the share of second-ranked South Korea) [29, p. 9].

U.S. enforcement action may prompt attackers to relocate their attack resources to countries where enforcement is weaker.[2] For instance, attackers might target their bots at computers in other countries, and even relocate their command-and-control servers. "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 suggests that many bot-infected computers in China are controlled from servers in other countries" [29, p. 36].

Figure 1 summarizes our theoretical model. We hypothesize that the number of attacks would be increasing in the Internet user population, decreasing in national government enforcement, increasing in national unemployment, and ambiguous in the number of published vulnerabilities. We further hypothesize that the number of attacks originating from *other countries* would be increasing in U.S. government enforcement and unemployment rate.

Our source of information about government enforcement was reports of enforcement in the news media. In the context of finance and accounting, news reports of corporate actions such as earnings, dividends, and mergers and takeovers have a significant, possibly temporary, impact on the corresponding share price within discrete time windows. Fama et al. [11] developed the event study methodology to measure the possibly temporary impact of reports of unanticipated corporate actions on stock market returns over a discrete time window.[3]

Our focus is the impact of enforcement and economic opportunities on Internet attacks rather than stock market returns. Accordingly, we adapted the event study methodology by applying linear regression with the number of Internet attacks as the dependent variable and news reports of enforcement events and unemployment as explanatory variables.[4] The specific model was

$$\log A_{it} = \alpha + \beta \log P_{it} + \gamma_1 \log U_{it} + \gamma_2 E_{it} + \gamma_3 \log U_{USt} \gamma_4 E_{USt} + \gamma_5 D_i + \eta \log V_t, \qquad (1)$$

where A_{it} is the number of attacks originating from country i at date t. The logarithmic specification is recommended for dependent variables that are positive and also serves to narrow the range of the dependent and explanatory variables, so reducing sensitivity of the estimates to extreme observations [30, pp. 198–199]. We detail the explanatory variables in Table 1.

The event day is that when government enforcement is first reported in the news media. A key issue in event studies is how to specify the "event window"—the period of time during which information might have an impact. The minimum event window is one day, being the day of the news report. The event window should be extended to take account of any disparity between the date of the actual event and the date of the corresponding news report.

Owing to broad interest, corporate actions are closely watched and reported in detail by multiple news media. Stock market event studies apply windows of one or three days. By contrast, information security attacks are likely to be of narrower interest and, so, less well covered by the general news media. Accordingly, we decided to use an event window of 15 days, comprising seven preevent days, the event day, and seven postevent days. Formally, if T_0 represented the event day, then the event window was $T_0 - 7$ to $T_0 + 7$. The seven preevent days would account for lags in news reports of enforcement action, whereas the seven postevent days would capture any delayed impact of enforcement. In robustness checks, we studied the sensitivity of our results to alternative definitions of the event window.

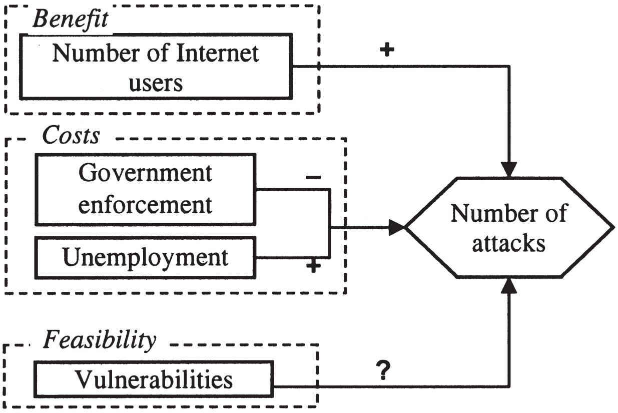

Figure 1. Internet Attack Model

Table 1. Explanatory Variables

Explanatory variable	Definition
P_{it}	Internet user population on an annual basis
U_{it}	National unemployment rate on a monthly basis
E_{it}	National enforcement event: $E_{it} = 1$ if within the event window, otherwise $E_{it} = 0$
U_{USt}	U.S. unemployment rate on a monthly basis
E_{USt}	U.S. enforcement event: $E_{USt} = 1$ if within the U.S. event window, otherwise $E_{USt} = 0$
D_i	Country-specific dummy variables, to control for unobserved time-constant but country-specific effects
V_t	Depreciated stock of vulnerabilities (since January 1, 2003), differentiated between high-, medium-, and low-risk levels—V_{ht}, V_{mt}, and V_{lt}, respectively.

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 they count only those attacks that meet a threshold of severity. The more serious limitation is that the ISC statistics only identify the originating country of the attacking packets by IP address, even though the originating computers may be under the remote control of attackers located in other countries.

The ISC provided country-level reports only from January 2004 onward.[5] We cut off our data collection on June 30, 2006. The sample period comprised 30 months or about 912 days. However, for unknown reasons, the 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 defined an event as any government enforcement action against Internet attackers. To identify the event of interest, we searched Factiva, a proprietary electronic database of news reports. 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; the key words 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 key words hack* and (convict* or sentence* or prosecut*) and the name of each of the sample countries.[6]

Following Symantec's definition of Internet security threats, we focused on enforcement actions against the following security breaches: malicious code (viruses, worms, Trojan horses, back door); spam; phishing; bots; denial of service; exploits of vulnerability; and security risks, including adware, spyware, misleading applications, and other unwanted programs. We excluded enforcement actions against violation of privacy and offline crimes such as physical sabotage, monitoring ATM users, and 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" [9]. If the same episode of enforcement was reported by more than one source, we simply counted the first source, and ignored later reports.

We also distinguished the reports of enforcement into three categories: enforcement without mention of fine or imprisonment (included mention of investigated, arrested, prosecuted, convicted, or community service), enforcement with fine, and enforcement with imprisonment.[7] However, the accuracy of the classification was subject to the detail reported by the media. For instance, an enforcement report from Japan on May 18, 2005, mentioned only "arrested." Hence, 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 the Organization for Economic Cooperation and Development (OECD),[8] and the National Statistical Bureau of Taiwan. It might be conjectured that Internet attacks are more closely related to unemployment among information technology (IT) professionals. For the United States, the Department of Labor reports the unemployment rate specific to the information industry, which comprises broadcasting, Internet service providers, Web search portals, and data processing services, motion picture and video, publishing,

Table 2. Sample Countries and Event Dates

Country	Number of sample days	Number of events	Earliest enforcement action report (year-month-day) (by penalty)*	
Australia	570	5	Prosecuted	20050914
			Convicted with fine only	20060214
			Convicted with jail only	20041014; 20050915; 20050917
Brazil	565	3	Probed	20040917
			Arrested	20050826
			Convicted with jail only	20040105
Canada	558	5	Arrested	20040528
			Prosecuted	20051117
			Convicted with jail only	20050106; 20060117; 20060125
France	548	12	Probed	20040526
			Arrested	20040605; 20041021; 20041223; 20050510; 20060616
			Prosecuted	20040513; 20060513
			Convicted with fine only	20040601; 20060331; 20060408
			Convicted with jail only	20060602
Germany	550	10	Probed	20041216; 20060511
			Arrested	20040317; 20060404
			Convicted with fine only	20060601
			Convicted with jail only	20040509; 20040514; 20040909; 20050706; 20050709
Great Britain	546	14	Arrested	20050128; 20050130
			Prosecuted	20040707; 20051105
			Convicted without fine or jail	20040202; 20040209
			Convicted with fine only	20051007
			Convicted with jail only	20040203; 20040623; 20040916; 20051008; 20051230; 20060117; 20060510

(continues)

Table 2. Continued

Country	Number of sample days	Number of events	Earliest enforcement action report (year-month-day) (by penalty)*	
Italy	545	27	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 only	20060331
Japan	546	6	Probed	20050414
			Arrested	20050518; 20051110; 20051129
			Convicted with jail only	20041119; 20050325
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 with fine only	20051016
			Convicted with jail only	20050929
Netherlands	545	3	Convicted without fine or jail	20051010
			Convicted with fine only	20041223
			Convicted with fine and jail	20050411

Poland	545	0	N.A.	
Spain	548	2	Convicted with jail only	20060213; 20060408
Sweden	544	8	Probed	0060302; 20060605
			Arrested	20050317; 20050511; 20050609
			Convicted with jail only	20050309; 20050401; 20050914
Taiwan	544	1	Convicted with jail only	20040528
United States	546	73	Probed	20060322; 20060515
			Prosecuted	20040301; 20040717; 20040817; 20050827
			Convicted without fine or jail	20040625; 20050225; 20050609; 20050802; 20060616
			Convicted with fine only	20040623
			Convicted with jail only	20040109; 20040223; 20040719; 20040805; 20040812; 20040907; 20041019; 20041215; 20041216; 20041217; 20041218; 20041223; 20050112; 20050129; 20050203; 20050212; 20050314; 20050315; 20050315; 20050415; 20050415; 20050505; 20050512; 20050611; 20050624; 20050907; 20050909; 20050914; 20051022; 20051229; 20060128; 20060301; 20060322; 20060413; 20060421; 20060506; 20060509; 20060510; 20060511; 20060516; 20060525; 20060608; 20060623
			Convicted with fine and jail	20040305; 20040326; 20040528; 20040713; 20040720; 20040824; 20041110; 20041231; 20050610; 20050816; 20051014; 20051202; 20060124; 20060213; 20060504; 20060507; 20060609; 20060626

* The events may not occur at the sample date.

software, and telecommunications. However, for the other countries, we had to use the overall unemployment rate.

We collected vulnerability data from the National Vulnerability Database (NVD), which is maintained by the Department of Homeland Security National Cyber Security Division/US-CERT. The NVD 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. Following the NVD, we categorized vulnerabilities according to their severity defined by the CVSS (Common Vulnerability Scoring System) score:[9] (1) high (CVSS 7–10), (2) medium (CVSS 4–6), and (3) low (CVSS 0–3). We compiled the total number of each category of published vulnerability on a daily basis. The number of vulnerabilities in each category varied over time but did not vary across countries.

As vulnerabilities published at earlier dates are more likely to have been patched by users, and thus less likely to enable successful attacks [3], we hypothesized that the number of attacks would depend on the *depreciated* stock of vulnerabilities to date. Accordingly, we constructed the depreciated stock with January 1, 2003, as the baseline as follows. For high-risk vulnerabilities, the depreciated stock at date *t* would be the weighted sum of the number of high-risk vulnerabilities published at each date during the period:

$$V_{ht} = \frac{1}{T} \sum_{k=1}^{T} v_{hk} k, \tag{2}$$

where v_{hk} is the number of high-risk vulnerabilities published at date *k* and *T* is the number of calendar days between January 1, 2003, and date *t*. The depreciated stocks of medium- and low-risk vulnerabilities, V_{mt} and V_{lt}, were defined in a similar way. Specification (2) gives higher weight to more recently published vulnerabilities. Table 3 provides summary statistics of the variables.

Empirical Results

Referring to Figure 1 and Equation (1), as a baseline, we regressed the number of attacks each day originating from each of the 15 countries on the explanatory variables other than U.S. unemployment and enforcement during the January 2004 to June 2006 period. The event window was seven days before and after the event day. Using ordinary least squares (OLS) without any adjustment of standard errors, the panel data exhibited high serial correlation ($F = 78.85$) and significant heteroskedasticity ($\chi^2 = 3.95$). Hence, we employed the robust covariance matrix estimator (a generalized White formula) to ensure consistency and efficiency [5, 10].

The results are reported in Table 4, column a. All of the estimated coefficients had the expected signs. Among them, the coefficient of enforcement was negative but insignificant, while the coefficient of national unemployment was positive but insignificant. Interestingly, the high-, medium-, and low-risk vulnerabilities had significantly

Table 3. Descriptive Statistics (15 Countries)

	Source	Total number of sample days	Minimum	Maximum	Mean	Standard deviation
Attacks	Internet Storm Center	8,245	1,706	23,200,000	1,298,673	2,358,852
Unemployment	OECD, Eurostat, etc.	8,245	3.20	19.80	7.27	3.59
Internet users	Euromonitor, Global Market Information Database	8,245	6,800	208,000	37,644.04	46,353.18
Vulnerability reports (by severity from low, medium, to high)						
Daily number						
High	National	8,245	0	139	4.25	9.87
Medium	Vulnerability	8,245	0	5	0.042	0.325
Low	Database	8,245	0	13	0.269	0.906
Cumulative stock with depreciation (since January 1, 2003)						
High		8,245	331.36	2,968.68	1,561.21	886.65
Medium		8,245	36.57	89.09	52.93	17.20
Low		8,245	212.11	303.78	254.65	26.10

		Period	Total number of events	Average number of events across countries	Standard deviation across countries
Enforcement news (by penalty)					
Probed	Factiva, Google, etc.	January 1, 2004	24	1.60	2.85
Arrested		to	30	2.00	2.42
Prosecuted		June 30, 2006	29	1.93	4.33
Convicted without fine or jail			8	0.53	1.36
Convicted with fine only			9	0.60	0.83
Convicted with jail only			73	4.87	10.72
Convicted with fine and jail			19	1.27	4.64
Total			192	12.80	18.40

Table 4. OLS Estimates (Dependent Variable: Number of Attacks Each Day)

	a	b	c	d	e	f	g (U.S. unemployment for information industry)	h (accelerated depreciation)
Time window (T_0 = event day)	$T_0-7\sim T_0+7$	$T_0-7\sim T_0+7$	T_0+7	$T_0-14\sim T_0+14$	T_0+14	$T_0-7\sim T_0+7$	$T_0-7\sim T_0+7$	$T_0-7\sim T_0+7$
Internet users	1.02984 (0.9956)	1.02174 (1.03246)	1.08888 (1.04298)	1.05105 (1.04383)	1.08684 (1.04512)	1.06880 (1.05404)	0.9588 (0.9934)	0.9601 (1.03229)
National enforcement	–0.000628 (0.04803)	–0.01327 (0.04818)	0.01068 (0.04997)	–0.02997 (0.05808)	–0.007866 (0.05944)	—	–0.02050 (0.05307)	0.006181 (0.04683)
National enforcement without fine or imprisonment	—	—	—	—	—	0.02131 (0.04548)	—	—
National enforcement with fine	—	—	—	—	—	–0.06570 (0.04225)	—	—
National enforcement with imprisonment	—	—	—	—	—	–0.07144 (0.08993)	—	—
U.S. enforcement	—	0.1316*** (0.02088)	0.07053*** (0.01778)	0.1300*** (0.03693)	0.04424 (0.02653)	—	0.1233**** (0.01626)	0.1194**** (0.01852)
U.S. enforcement without fine or imprisonment	—	—	—	—	—	0.1904**** (0.02686)	—	—

U.S. enforcement with fine	—	—	—	—	—	0.003082	—	—
						(0.02266)		
U.S. enforcement with imprisonment	—	—	—	—	—	0.07582	—	—
						(0.02303)***		
National unemployment rate	0.4214	0.3179	0.3691	0.3396	0.3681	0.3966	0.3878	0.2593
	(0.6882)	(0.6803)	(0.6979)	(0.6823)	(0.6891)	(0.7034)	(0.6714)	(0.6201)
U.S. unemployment rate	—	2.9236***	3.1855***	3.3710***	3.3068***	2.9448***	0.2888***	3.2584**
		(0.8977)	(0.8737)	(0.8662)	(0.8704)	(0.8632)	(0.08001)	(1.2277)
High-risk vulnerabilities	0.9799****	1.026****	1.099****	1.167****	1.137****	1.010****	0.7152***	0.9421****
	(0.2306)	(0.1837)	(0.1840)	(0.1991)	(0.1781)	(0.1813)	(0.2055)	(0.1521)
Medium-risk vulnerabilities	1.519**	1.189**	1.318**	1.490***	1.411***	1.040**	0.8340	0.1212
	(0.5467)	(0.4616)	(0.4596)	(0.4837)	(0.4602)	(0.4497)	(0.4987)	(0.1933)
Low-risk vulnerabilities	3.872****	3.267****	3.188****	3.076****	3.096****	3.525****	3.521****	2.010****
	(0.8296)	(0.7467)	(0.7508)	(0.7431)	(0.7544)	(0.7634)	(0.8629)	(0.2397)
Constant	–31.68**	–31.99**	–33.66**	–34.18**	–33.96**	–33.30**	–24.98**	–18.49
	(10.78)	(12.04)	(12.03)	(12.00)	(12.01)	(12.49)	(10.81)	(10.59)
Number of observations	8,245	7,699	7,699	7,699	7,699	7,699	7,699	7,699
Adjusted R^2	0.6828	0.4918	0.4886	0.4894	0.4876	0.4948	0.4876	0.5032
Impact of national enforcement (in percent)[1]	–0.18	–1.43	0.95	–3.12	–0.96	2.05	–2.17	0.51
	(±4.79)	(±4.75)	(±5.04)	(±5.62)	(±5.88)	(±4.64)[2]	(±5.19)	(±4.70)
						–6.44		
						(±3.95)[3]		
						–7.27		
						(±8.32)[4]		

(continues)

Table 4. Continued

	a	b	c	d	e	f	g (U.S. unemployment for information industry)	h (accelerated depreciation)
Time window (T_0 = event day)	$T_0-7\sim T_0+7$	$T_0-7\sim T_0+7$	T_0+7	$T_0-14\sim T_0+14$	T_0+14	$T_0-7\sim T_0+7$	$T_0-7\sim T_0+7$	$T_0-7\sim T_0+7$
Impact of U.S. enforcement (in percent)[1]	—	14.04 (±2.38)	7.29 (±1.91)	13.81 (±4.20)	4.49 (±2.77)	20.93 (±3.25)[5] 0.28 (±2.27)[6] 7.85 (±2.48)[7]	13.10 (±1.84)	12.66 (±2.09)
Impact of U.S. unemployment (in percent)[8]	—	0.04	0.05	0.05	0.05	0.04	0.23	0.05

Notes: All variables in logarithm, except enforcement. All standard errors robust to heteroskedasticity and serial correlation within country. [1] The effects and corresponding standard errors of dummy variables were calculated by using equation 1.4 in Kennedy [17, p. 801] and equation 2.4 in Garderen and Shah [13, p. 152]. [2] The impact of national enforcement without fine or imprisonment. [3] The impact of national enforcement with fine. [4] The impact of national enforcement with imprisonment. [5] The impact of U.S. enforcement without fine or imprisonment. [6] The impact of U.S. enforcement with fine. [7] The impact of U.S. enforcement with imprisonment. [8] This row presents the percentage impact on the number of attacks caused by every 1,000-person increase in the U.S. unemployed in general or in the information industry, which was calculated by {[1 + 1,000/the number of the total unemployed]^the estimated coefficient of the U.S. unemployment rate}. In 2006, the number of all unemployed persons at least age 16 was 7,001,000, while the number of unemployed persons in the information industry at least age 16 was 126,000 (U.S. Department of Labor, *Current Population Survey;* www.bls.gov/cps/). **** significant at 99.9 percent; *** significant at 99 percent; ** significant at 95 percent; * significant at 90 percent.

positive effects on the number of attacks. The effect of the low-risk vulnerabilities was the highest followed by the medium- and high-risk vulnerabilities. This was possibly because software vendors spent more effort developing patches for and end users were more diligent in fixing high-risk vulnerabilities than lower-risk vulnerabilities. Then attackers would have been motivated to target lower-risk vulnerabilities.

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 of the estimated coefficients had the expected signs.

In Table 4, the third and next to last rows report effects of U.S. or national enforcement and the corresponding standard errors as calculated by using equation 1.4 in Kennedy [17, p. 801] and equation 2.4 in Garderen and Shah [13, p. 152]. Interestingly, both the U.S. unemployment rate and enforcement were associated with significantly positive effects on the number of attacks originating from other countries. On average, a U.S. enforcement action was associated with a 14.04 percent (±2.38 percent) 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 national enforcement on the number of attacks increased in absolute value from –0.18 percent (±4.79 percent) in specification (a) to –1.43 percent (±4.75 percent) in specification (b), but was still insignificant.

In Table 4, the last row reports the impact of U.S. unemployment on the number of attacks. Specifically, an increase in the number of U.S. unemployed by 1,000 persons was associated with the number of attacks being 0.04 percent higher.

These results provided evidence for the existence of a cross-boundary *displacement effect* of enforcement actions. Specifically, announcement of U.S. enforcement against Internet security violators might persuade perpetrators to relocate their bots, and possibly their command-and-control servers, to other countries where enforcement is weaker.

To check the robustness of our results, we reestimated Equation (1) with various alternative event windows: only seven days after the event day, 14 days before and after the event day, and 14 days after the event day. Table 4, columns c, d, and e, respectively, report the results. The coefficients of all variables except national enforcement had the expected signs with only slight change in magnitude.

There was some evidence that both national and U.S. enforcement had an effect before the publication of the corresponding news report. Specifically, the displacement effect of U.S. enforcement was 14.04 percent (±2.38 percent) with the event window of seven days before and after the event day (as reported in Table 4, column b) as compared to 7.29 percent (±1.91 percent) with the event window of seven days after the event day, as reported in Table 4, column c. Likewise, the displacement effect of U.S. enforcement was 13.81 percent (±4.20 percent) with the event window of 14 days before and after the event day (as reported in Table 4, column d) as compared to 4.49 percent (±2.77 percent) with the event window of 14 days after the event day (as reported in Table 4, column e).[10] These results suggest that either information about the enforcement leaked out ahead of the media report or media reports were delayed.

Table 4, column f, reports estimates with the finer indicators of enforcement—enforcement without imprisonment or fine, enforcement with fine, and enforcement with imprisonment. As expected, for both national enforcement and U.S. enforcement, the deterrent effect of imprisonment on attacks was much larger than that of fines. The impact from the national enforcement without imprisonment or fine was much smaller in magnitude and even insignificantly positive. Surprisingly, the impact of U.S. enforcement without imprisonment or fine was relatively large. This counterintuitive result may be due to the much smaller number of enforcement events without imprisonment or fine compared to enforcement events with imprisonment in the studied period as shown in Table 2.

We next addressed the robustness of the results to measures of unemployment and the stock of vulnerabilities, and the estimation method. First, attackers are likely to come from a specialized segment rather than the general population. Hence, the overall unemployment rate may not accurately reflect the economic opportunities for attackers. In Table 4, column g, we replaced the U.S. overall unemployment rate with the unemployment rate specific to the information industry. This change did not affect the estimated coefficients very much. The impact of the U.S. enforcement events became slightly smaller than that of specification (b). In particular, an increase in the number of unemployed in the U.S. information industry by 1,000 persons was associated with a 0.23 percent increase in the number of attacks originating from other countries. The impact is much higher than the 0.04 percent increase in attacks arising from an increase in the U.S. overall unemployed by 1,000. These results are consistent with the thinking that unemployed IT professionals are a major source of Internet attacks.

Second, we considered an alternative measure of the stock of vulnerabilities, which provided for faster depreciation:

$$V_{ht} = \frac{1}{T^2} \sum_{k=1}^{T} v_{hk}^2 k. \tag{3}$$

The results are reported in Table 4, column h. Compared to column b, there was a slight difference in the impact of U.S. enforcement and unemployment. The major difference was that the coefficients of the stocks of high-, medium-, and low-risk vulnerabilities were smaller, which suggests that attackers did pay attention to vulnerabilities published earlier.

Third, like Campbell et al. [6], we used seemingly unrelated regressions to examine whether 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 99.9 percent level (χ^2 = 53.80). However, we could not reject the null hypothesis that the coefficient of U.S. enforcement was the same across countries (χ^2 = 3.98). This is further evidence that the brains behind the attacks were situated in the United States and they relocated attack sources in response to U.S. government enforcement.

Finally, we addressed concerns that heteroskedasticity and serial correlation arise in such studies [5, 10]. The OLS estimates in Table 4 were reported with robust standard errors. Besides, we also checked that our findings were robust to estimation by feasible general least squares (FGLS) with heteroskedastic and panel-specific autocorrelation error structure. The results were consistent with the findings presented in Table 4, column b.

Alternative Methodology

The impact of enforcement actions on Internet attacks could also be measured by directly adapting the event study methodology from financial economics [22]. This approach would construct a statistical 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 three serious shortcomings. First, it works well only for events that take place quickly, such as an enforcement action. It cannot be used to study the impact of longer-term variables such as unemployment, which are reported only monthly or at longer intervals.

The two other shortcomings were econometric. One is the requirement of an uncontaminated estimation period [2]. Several of the enforcement events listed in Table 2 occurred close in time, resulting in an overlap between the estimation period of one event and the event windows of other events. Discarding such events would reduce the power of our statistical tests. Further, our study used cross-country time-series data, and as mentioned above, was subject to cross-country heteroskedasticity and serial correlation within countries.

Notwithstanding the limitations, 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 nine.[11]

The estimates showed that in the United States, Great Britain, Italy, and Sweden, reports of government enforcement were associated with an average 12 percent reduction in the number of Internet attacks within an event window of one week before and after the event day. This effect was statistically significant. These four countries accounted for more than 68 percent of the enforcement actions and 86 percent of sentences of imprisonment among the nine countries. However, for the other five countries, the effect of enforcement was ambiguous.

Concluding Remarks

We made three contributions. First, we adapted the event study methodology from research in financial economics to another context where high-frequency data on the variable of interest is available. The preferred methodology uses linear regression with the number of attacks as the dependent variable and indicators of enforcement events as explanatory variables.

Our second contribution was the empirical finding that U.S. enforcement and unemployment had a substantial displacement effect on Internet attacks. Increases in U.S.

enforcement and unemployment were associated with substantial increases in attacks originating from other countries. The implication for government policy is that, in a networked world, national enforcement is not sufficient to deter cyber criminals. International cooperation in enforcement is essential.

Our empirical results also provide some evidence in favor of delayed publication of vulnerabilities. We found that Internet attacks increased with the number of published vulnerabilities. The policy implication is that, if users do not quickly patch vulnerabilities, social welfare might be higher with delayed publication of vulnerabilities.

Our findings are subject to several limitations. First, they are limited to economically motivated attacks on information security. They might not apply to the activities of teenage hackers motivated by curiosity or peer approval. Second, ISC statistics only identified the originating country of the attacking packets by IP address, although the originating computers might be remotely controlled from other countries. Third, our dependent variable was all attacks for each country. Future research should aim to identify the ultimate source of attacks (the location of the controlling server) and classify attacks in an appropriate way (e.g., the computer port) and associate them with the corresponding vulnerabilities.

Acknowledgments: The authors gratefully acknowledge financial support from the U.S. Air Force Asian Office of Aerospace R&D (award FA4869–07–1-4046), the Academic Research Fund (grant R-313–000–076–112), and the School of Computing in the National University of Singapore. They thank Eric Clemons, Rajiv Dewan, Rob Kauffman, *JMIS* reviewers, Forty-First Annual Hawaii International Conference on System Sciences Competitive Strategy, Economics and IS mini-track reviewers, Seventh Workshop on the Economics of Information Security participants, and Larry Gordon for valuable suggestions and comments.

Notes

1. This variable—the Internet user population—also serves to control for any correlation between macro-economic variables such as unemployment and the number of attacks due to purely macro-economic factors.

2. In the context of crime in general, economic analyses have hypothesized that security measures may cause crime to be displaced [18].

3. Generally, the measured impact, which is called the “abnormal return,” is the difference between the return on the stock with the unanticipated change in information, i.e., the actual return, less the return without the change in information, as forecast by a statistical model (see, for instance, [22]). The event study methodology has been variously applied to study the stock market impact of breaches of information security [1, 6, 7].

4. The most direct adaptation of the event study methodology would be to construct a statistical 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 below, this approach suffers serious limitations in the information security context.

5. The country-level number of reports published by the ISC was defined as the average number of packets reported from each IP address in the respective country.

6. Reports in each of the various languages were compiled by coders specializing in the respective language. However, owing to resource limitations, the reports were not checked by a second coder.

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

8. See http://ec.europa.eu and http://stats.oecd.org/WBOS/Index.aspx?QueryName=252&QueryType=View.

9. CVSS is designed to rank information system vulnerabilities and provide the end user with a composite score representing the overall severity and risk presented by the vulnerability.

10. Similarly, the deterrent effect of national enforcement was –1.43 percent (±4.75 percent) with the event window of seven days before and after the event day (as reported in Table 4, column b) as compared to 0.95 percent (±5.04 percent) with the event window of seven days after the event day (as reported in Table 4, column c). The magnitude of the deterrent effect also became smaller when the event window changed from 14 days before and after the event day to 14 days after the event day—that is, from –3.12 percent (±5.62 percent) (as reported in Table 4, column d) to –0.96 percent (±5.88 percent) (as reported in Table 4, column e).

11. Australia, Brazil, Spain, Netherlands, Poland, and Taiwan (China) were excluded.

References

1. Acquisti, A.; Friedman, A.; and Telang, R. Is there a cost to privacy breaches? An event study. Paper presented at the Fifth Workshop on the Economics of Information Security (WEIS), Cambridge, UK, June 26–28, 2006.

2. Aktas, N.; de Bodt, E.; and Cousin, J.G. Event studies with a contaminated estimation period. *Journal of Corporate Finance, 13,* 1 (2007), 129–145.

3. Arora, A.; Nandkumar, A.; and Telang, R. Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontier, 8,* 5 (2006), 350–362.

4. Becker, G. Crime and punishment: An economic approach. *Journal of Political Economy, 76,* 2 (March–April 1968), 169–217.

5. Bertrand, M.; Duflo, E.; and Mullainathan, S. How much should we trust differences-in-differences estimations? *Quarterly Journal of Economics, 119,* 1 (February 2004), 249–275.

6. Campbell, K.; Gordon, L.A.; Loeb, M.P.; and Zhou, L. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11,* 3 (2003), 431–448.

7. 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. *International Journal of Electronic Commerce, 9,* 1 (Fall 2004), 70–104.

8. Choi, J.P.; Fershtman, C.; and Gandal, N. Internet security, vulnerability disclosure, and software provision. Working paper, Michigan State University, East Lansing, July 2006.

9. DoD hacker sentenced to 21 months hard Time. *Information Week* (May 12, 2005).

10. Donald, S.G., and Lang, K. Inference with difference-in-differences and other panel data. *Review of Economics and Statistics, 89,* 2 (2007), 221–233.

11. Fama, E.F.; Fisher, L.; Jensen, M.C.; and Roll, R. The adjustment of stock prices to new information. *International Economic Review, 10,* 1 (1969), 1–21.

12. Freeman, R.B. The economics of crime. In O. Ashenfelter and D.E. Card (eds.), *Handbook of Labor Economics,* volume 3C. Amsterdam: Elsevier, 1999, pp. 3529–3571.

13. Garderen, K.J.V., and Shah, C. Exact interpretation of dummy variables in semilogarithmic equations. *Econometrics Journal, 5,* 1 (2002), 149–159.

14. Heal, G., and Kunreuther, H. Interdependent security: A general model. Working paper 10706, National Bureau of Economic Research, Cambridge, MA, August 2004.

15. Jordan, T., and Taylor, P. A sociology of hackers. *Sociological Review, 46,* 4 (1998), 757–780.

16. Kannan, K., and Telang, R. Market for software vulnerabilities? Think again. *Management Science, 51,* 5 (2005), 726–740.

17. Kennedy, P.E. Estimation with correctly interpreted dummy variables in semilogarithmic equations. *American Economic Review, 71,* 4 (1981), 801.

18. Koo, H.W., and Png, I.P.L. Private security: Deterrent or diversion? *International Review of Law and Economics, 14,* 1 (1994), 87–101.

19. Kshetri, N. The simple economics of cybercrimes. *IEEE Security & Privacy, 4,* 1 (January–February 2006), 33–39.

20. Kunreuther, H., and Heal, G. Interdependent security. *Journal of Risk and Uncertainty, 26,* 2–3 (2003), 231–249.

21. Lee, D., and McCrary, J. Crime, punishment, and myopia. Working paper no. W11491, National Bureau of Economic Research, Cambridge, MA, July 2005.

22. Mackinlay, A.R. Event studies in economics and finance. *Journal of Economic Literature, 35,* 1 (1997), 13–39.

23. Mell, P.; Scarfone, K.; and Romansky, S. CVSS: A complete guide to the common vulnerability scoring system version 2.0. *First.org* (June 2007) (available at www.first.org/cvss/cvss-guide.html).

24. Png, I.P.L.; Tang, C.Q.; and Wang, Q.H. Hackers, users, information security: Welfare analysis. Paper presented at the Fifth Workshop on the Economics of Information Security (WEIS), Cambridge, UK, June 26–28, 2006.

25. Polinsky, A.M., and Shavell, S. The economic theory of public enforcement of law. *Journal of Economic Literature, 38,* 1 (March 2000), 45–77.

26. Raphael, S., and Winter-Ebmer, R. Identifying the effect of unemployment on crime. *Journal of Law and Economics, 44,* 1 (April 2001), 259–284.

27. Romania: New citadel of cybercrime. *CBS News* (October 20, 2003) (available at www.cbsnews.com/stories/2003/10/20/tech/main578965.shtml).

28. Symantec Internet security threat report: Trends for January 05–June 05, vol. VIII. Symantec, Cupertino, CA, September 2005 (available at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_viii.pdf).

29. Symantec Internet security threat report: Trends for July–December 06, vol. XI. Symantec, Cupertino, CA, March 2007 (available at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf).

30. Wooldridge, J.M. *Introductory Econometrics: A Modern Approach,* 3d ed. Mason, OH: Thomson Higher Education, 2006.