Singapore Management University

Institutional Knowledge at Singapore Management University

Research Collection School Of Computing and Information Systems

School of Computing and Information Systems

2012

Reputation as Public Policy for Internet Security: A Field Study

Qian TANG
Singapore Management University, QIANTANG@smu.edu.sg

Leigh L. Linden

John S. Quarterman

Andrew Whinston

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research

Part of the Computer Sciences Commons, and the E-Commerce Commons

Citation

TANG, Qian; Linden, Leigh L.; Quarterman, John S.; and Whinston, Andrew. Reputation as Public Policy for Internet Security: A Field Study. (2012). *International Conference on Information Systems (ICIS), December 2012, Orlando, FL*.

Available at: https://ink.library.smu.edu.sg/sis_research/1844

This Presentation is brought to you for free and open access by the School of Computing and Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Computing and Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email cherylds@smu.edu.sg.

REPUTATION AS PUBLIC POLICY FOR INTERNET SECURITY: A FIELD STUDY

Completed Research Paper

Qian Tang
University of Texas at Austin
2110 Speedway, B6500
Austin, TX 78712
qian.tang@phd.mccombs.utexas.edu

Leigh Linden
University of Texas at Austin
2225 Speedway, C3100
Austin, Texas 78712
leigh.linden@austin.utexas.edu

John S. Quarterman
Quarterman Creations
3338 Country Club Road #L336
Valdosta, GA 31605
jsq@quarterman.com

Andrew B. Whinston
University of Texas at Austin
2110 Speedway, B6500
Austin, TX 78712
abw@uts.cc.utexas.edu

Abstract

Cybersecurity is a national priority in this big data era. Because of the lack of incentives and the existence of negative externality, companies often underinvest in addressing security risks and accidents, despite government and industry recommendations. In the present article, we propose a method that utilizes reputation through information disclosure to motivate companies to behave pro-socially, improving their Internet security. Using outbound spam as a proxy for Internet security, we conducted a quasi-experimental field study for eight countries through SpamRankings.net. This outgoing-spam-based study shows that information disclosure on outgoing spam can help reduce outgoing spam, approximately by 16 percent. This finding suggests that information disclosure can be leveraged to encourage companies to reduce security threats. It also provides support for public policies that require mandatory reporting from organizations and offers implications for evaluating and executing such policies.

Keywords: Security, public policy, filed study, quasi-experiment, reputation, incentive

Introduction

The year of 2011 was a busy one for cyber attacks on many organizations, with targeted attacks increasing by 400 percent. Industries such as credit card companies, gaming platforms, banks, retailers, TV networks, and government agencies, all fell victim to cyber crimes, which have not only increased in frequency but also in the severity of damage. According to Ponemon Institute, the median cost caused by cyber crimes is $5.9 million per year per company, with a range from $1.5 million to $36.5 million. The costs consist of both direct expenses (recovery, detection, etc.) and indirect costs (information loss, business disruption, revenue loss, equipment damages, etc.). However, the study by Ponemon Institute also indicates that nearly all of these attacks were avoidable. Although most attacks were targeted, the target selection was based more on opportunity than on choice. Most organizations fell victims not because they were pre-identified but because they were found to possess exploitable vulnerabilities. About 50%-75% of security incidents originated from within an organization (D'Arcy et al. 2009). Ninety-six percent of victim organizations subject to PCI DSS1 were not in compliance with the standards. Most attacks were carried out using fairly simple methods and could have been stopped easily with basic or intermediate controls.

This observation reflects that, besides technology availability, some fundamental problem needs to be solved to create a secure cyber environment. The current situation is that although security has become a general concern, organizations still hesitate to invest sufficiently in security controls because they often consider information security too expensive to achieve. Security products and services are sometimes regarded as useful and desirable yet not affordable. High-level security practices can be reinforced to prevent security disasters and control the damage. The deployment of such practices, however, is a costly endeavor for organizations without assured significant benefit. With the proliferation of mobile devices, the increasing number of locations and devices where information can be stored further adds to the cost for prevention and protection. Given the rising costs, the rewards for security and the penalties for security failure remain relatively low. Besides, it is difficult to measure the risk and potential costs of security breaches beforehand. While data breach disclosure laws generally require companies to notify individuals when their personal information has been lost or stolen, they can choose not to reveal publicly any data breach or cyber attacks to reputation loss. The lack of transparency enables organizations to claim to be secure even if their system configurations are in fact vulnerable. Customers and business partners, who also bare the security risk with the organization, lack information to evaluate the potential costs for themselves beforehand. Moreover, organizations tend to ignore the negative externalities of their security vulnerabilities on other organizations. The security vulnerabilities of an organization are often used against other organizations. For example, botnets opportunistically scan the Internet to find and compromise systems with exploitable weaknesses. These compromised computers are then utilized to collectively attack other targeted systems by ways including spamming. The vulnerabilities may also be exploited for information theft or to stage a denial of service attack.

While focusing on technical solutions, existing studies often tend to ignore the fundamental incentive issue. As economic gains have made hacking a lucrative business for criminals in the underground economy, organizations lack strong incentives to give security top priority. We propose that organizations' incentives to increase security spending can be enhanced through information disclosure, especially public information disclosure. As aforementioned, the lack of incentive is due to the lack of transparency and the existence of negative externality. Public information disclosure can create a transparent environment where customers and business partners are informed of the organization's security issues. More importantly, through public information disclosure, we can build a reputation system where organizations are evaluated against their security responsibilities. Information can be gathered either through third-party monitoring mechanisms or public policies that require mandatory reporting from organizations (Quarterman et al. 2011). In academia, it has been recognized that a key factor required to improve Internet security is the gathering, analysis, and sharing of information related to security issues (Gal-Or and Ghose 2005). In practice, the Securities and Exchange Commission (SEC) formally asked public companies to disclose cyber attacks against them in October 2011. However, mandatory disclosure prior to cyber attacks can more effectively draw the attention of both the chief executives and the public, and encourage enhanced protection against cyber attacks. The way the information is presented to the public is crucial once it has been gathered. Without comparisons with other businesses, the isolated information disclosed about an organization does not provide a clear evaluation. Aggregating information from different organizations and presenting it in a way that allows easy comparisons would be more meaningful for the public. Therefore, what we propose in this paper is not only public information disclosure but also information aggregation and presentation. Relative performance ranking can be more effective in inducing peer influence from other organizations and thus imposing reputation incentives on the subject organization.

We conducted a field study to evaluate the effect of public information disclosure and presentation. Specifically, we disclosed security information for organizations in the treatment group but not for organizations in the comparison group. The field setting ensures that organizations and the public behave in a natural manner, and the quasi-experimental manipulation introduces exogenous variation only in information disclosure. Sample organizations were observed for several periods during which we collected data repeatedly, and the panel allowed us to evaluate the effect of public information disclosure dynamically. The results show that organizations exposed to public disclosure of security issues tend to become more secure than organizations without information disclosure. The results provide empirical support for public policies on information disclosure of security issues.

Our approach for improving Internet security is complementary to existing technical approaches. The vast technical literature, especially in the computer science area, has focused on the development of technologies to secure computer systems, such as secure networking protocols, intrusion detection techniques, database security methods, and access control technologies (Ransbotham and Mitra 2009). By focusing on organizations' incentives to invest in these technologies, we aim to extend prior work and provide a more comprehensive lens for studying Internet security. Our study sheds light on public policy issues concerning security information report and disclosure, and provides a new perspective for dealing with environmental issues such as pollution, energy saving, and carbon dioxide emissions, where externality leads to lack of incentives for taking pro-social behavior.

Literature Review

Information Security

Existing literature on information security focuses on organizational strategies that can be used for reducing system risk, including deterrence, prevention, detection, and recovery (Forcht 1994, Straub and Welke 1998). For deterrence and prevention, most previous studies, from the organizational perspective, examine the impact of security policy and practice on information systems abuse or misuse. Straub (1990) found that security policy statements and technical controls were associated with lower levels of computer abuse. Kankanhalli et al. (2003) found that more time spent on security activities and more advanced security software used were associated with higher perceived security effectiveness. D'Acy et al. (2009) found that user awareness of security policies, security education, training, and awareness (SETA) programs, and computer monitoring can deter information systems misuse. For detection and recovery, research has been focused on how to identify attack traffic that could originate from both internal and external sources in a cost effective way. Toth and Kruegel (2002) proposed a framework to automate the selection process of the best response action by minimizing negative security costs. Carver and Pooch (2000) added the attacker's degree of suspicion, the timing of the attacks, and the environmental constraints as the relevant factors for response selection. Yue and Cakanyildirim (2007) studied the response decision for intrusion detection and showed that the choice of an optimal mixture of reactive and proactive responses depends on the values of cost parameters and investigation rate parameters. Mookerjee et al. (2011) proposed a detection approach for systems that operate under conditions where the miscreants can modify their behavior depending on the state of the system.

Security vulnerability disclosure is an area of public policy that has been subject to considerable debate (Arora et al. 2004b). Studies on software vulnerability disclosure showed that while disclosing vulnerability information provides an impetus to the vendor to release patches early, instant disclosure leaves users defenseless against attackers who can exploit the disclosed vulnerability (Elias 2001 and Farrow 2000). Arora et al. (2004a) found that while vendors are quick to respond to instant disclosure, vulnerability disclosure also increases the frequency of attacks. Arora et al. (2004b) suggested that the optimal vulnerability disclosure depends upon underlying factors such as how quickly vendors respond to disclosure by releasing patches and how likely attackers are to find and exploit undisclosed or unpatched vulnerabilities. Although there has been no public disclosure on information security vulnerability, industry-based Information Sharing and Analysis Centers (ISACs), where security breach information is revealed to information-sharing alliance, has been established to facilitate the sharing of security information to enhance and protect critical cyber infrastructure. Gal-Or and Ghose (2005) studied the economic incentives for security information sharing and found that information sharing yields greater benefits in more competitive industries. Gordon et al. (2003) examined how information sharing affects the overall level of information security when firms face the trade-off between improved information security and the potential for free riding. By studying security information disclosure to the public, we aim to extent prior work and provide a more comprehensive evaluation for public policy.

Incentives

It has long been recognized by many researchers that Information security is not a problem that technology alone can solve (Arora et al. 2004a). Anderson (2001) proposed that information insecurity is due to perverse incentives, which are distorted by network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the so-called tragedy of the commons. Schneier (2002) also argued that often systems fail because of misplaced economic incentives: The people who could protect a system are not the ones who suffer the costs of failure. According to these studies, many security questions are at least as much economic as technical. It has been realized that security failure is caused at least by bad incentives as by bad design (Anderson and Moore, 2006). These previous studies are highly informative and provide the groundwork for the current analysis.

In this study, we leverage three incentive mechanisms to improve information security: concerns for security breach, reputation (fame or shame), and peer influence. First, firms are generally concerned about security threats. Public security information disclosure can help raise the organization's awareness of its security vulnerabilities. Second, security information disclosure can make firms feel ashamed of their irresponsibility for the overall Internet security. Shame is triggered by a choice made in public that does not maximize the payoffs of others (Satio 2011). Dillenberger and Sadowski (2010) suggested that a person's behavior may depend on whether it is observed by someone who is directly affected by it and shame is a moral cost for a person's utility. These concepts can be extended to organizational behavior since organizations are also concerned about their social image and responsibilities (Frei 2010). Third, the most important incentive for organizations to take positive reaction to information disclosure is peer influence through comparison with others, especially their competitors. With the increasing concern for privacy and confidentiality, customers would choose or switch to firms with a more secure information system. Social comparison theory (Festinger 1954) indicates that publicly comparing similar organizations can change their behaviors through peer pressure. Luttmer (2005) demonstrated that, controlling for an individual's own income, higher earnings of neighbors are associated with lower levels of self-reported happiness. For organizations, we expect peer pressure to be more prominent because of competitions.

Regulations on Information Disclosure

Security information disclosure laws have been focused on data breach notification. Although a national data-breach notification law is still in the air, as of August 20, 2012, 46 U.S. states and the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information (NCSL, 2012). The specific requirements of notification laws vary across states. Some laws require notification when the personal information is reasonably assumed to have been acquired by an unauthorized party, whereas others require notification only if it is reasonable to believe the information will cause harm to consumers. The consequences of not complying differ from state to state as well. However, the rationales for these laws are consistent, which is also consistent with our rational for public disclosure of security vulnerabilities, that notification can provide public information and create an incentive for all firms (even those that have not been breached) (Ponemon Institude 2005, Schwartz & Janger 2007, Romanosky et al. 2011).

However, the impact of data breach disclosure is still in debate. The concerns include: (1) firms must comply with multiple, disparate, and perhaps conflicting state laws (Romanosky et al 2011); (2)

notifications simply shift the burden to consumers if breaches really cause harm (Lenard and Rubin 2005, 2006, Cate 2009). Otherwise, they are just unnecessary costs. Romanosky et al. (2011) found that data breach disclosure can reduce identity theft caused by data breaches. Campbell et al. (2003) found a highly significant negative impact of security breaches reported in newspapers on the stock price of the breached company only when the breach involves unauthorized access to confidential data. In contrast, Kannan et al. (2007) found security breach announcements have no significant negative impact on market return in the long run.

The impact of information disclosure has also been widely studied in areas other than security. Jin and Leslie (2003) studied health information disclosure in the restaurant industry and found that disclosing the hygiene quality information increases health inspection scores and lowers certain diseases. Cain et al. (2005) examined the effect of disclosing conflicts of interest and found the disclosure can have perverse effects because advice receivers do not discount advice sufficiently and advice givers exaggerate advice even further. Other information disclosure studies are related to auto safety, public education, and so on (Fung et al. 2007). These studies provide some evidence of how information disclosure can affect firm behavior. Based on these studies, we further add the aggregation and presentation of information, which can leverage reputation and peer influence to enhance disclosure effect.

Field Study

Field experimentation has been used extensively for policy evaluation (Duflo et al. 2010). It has also been used to study information security and privacy (Hui et al. 2007). These experimental studies randomly assign participants into treatment groups or control groups. Randomization, although more desirable in ideal environment, is inappropriate given our circumstance. In this study, we aim to evaluate whether public information disclosure can lead to security improvement. A typical field experiment design is to select certain geographic areas, mandate organizations within these areas to report on their security issues, and disclose the reported information to the public. Such an ideal experiment has to be done with policy enforcement from the government, which is very expensive and time consuming. In our study, we are able to utilize current technologies to collect information without mandatory reporting and impose treatment without policy enforcement. Without policy enforcement, publicity of the disclosed information is critical to the success of the study. To make sure our disclosed information can draw sufficient attention from the public, we limit the treated originations to be North American or Europe based, considering the authors' PR connections. We further use a quasi-experimental design to find control groups.

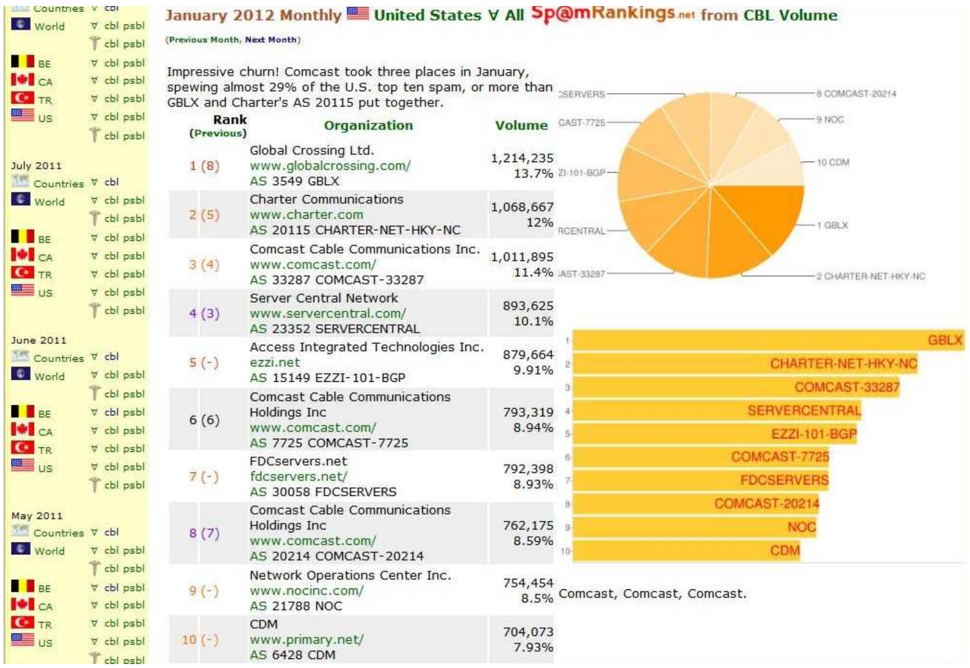
Outgoing Spam as Proxy for Internet Security

Although Internet security has many aspects, we focus on outgoing spam, or the unsolicited bulk email, which includes the Unsolicited Commercial Email (UCE). Most spam messages are sent by botnets, a collection of compromised computers (bots) controlled by a bot herder who rents access to them for sending spam or other miscreant purposes. Anti-spam blocklists have spam traps scattered across the Internet and can recognize similar messages received at multiple locations. Inbound spam refers to the spam received, and many organizations can filter spam out of incoming emails before their employees or users see it. However, they usually do nothing to stop outbound spam originating from computers within the organizations. Outbound spam is typically generated via zombie computers, compromised user accounts, or spammers who knowingly abuse their accounts (e.g., in snowshoe spam), and is often considered as a proxy for Internet security because it is a common symptom of more damaging security problems (Quarterman et al. 2010). The same vulnerabilities that enable spam are also openings for other exploits. For example, miscreants can steal existing accounts by tricking end-users (through phishing or by human engineering) into providing their email usernames and passwords. Such stolen accounts can then be used to install botnet spamming malware, or other exploits such as Distributed Denial of Service (DdoS) software or sniffers, causing theft of customer records and intellectual property, fraudulent use of corporate online banking, or even employee blackmail.

It is costly to deal with outbound spam, which often leads to major side effects such as IP blocking by RBL, DNSBL, and IP reputation systems. This causes queue buildup on the affected mail server, delays in message delivery, and may result in lost messages and calls from unhappy end-users. It also leads to compromised user accounts and blocking of legitimate outbound email, which then cause damage to reputation, customer relationship, business operation, and eventually lower profit. Unfortunately, conventional anti-spam measures may not work well for outbound traffic. Internet service providers (ISPs) are constantly fighting against inbound spam, phishing and email-borne malware, and are generally well equipped to cope with inbound spam. However, they might be unaware of the fact that they could also be the sources of malicious emails. Their customers are usually not informed until a serious attack occurs. Therefore, if ISPs are constantly sending out spam, they not only risk being attacked themselves but also increase the risk faced by other Internet users. Hence outbound spam is a typical Internet security problem that lacks transparency, can cost a lot to deal with, and imposes negative externality for other Internet users. If public information disclosure proves effective in reducing outgoing spam, it can also be used for reducing problems in other security dimensions.

SpamRankings.net

We launched a website named SpamRankings.net in May 2011 and have since used it to disclose outbound spam information. This website serves as our main instrument to study public security information disclosure and presentation. It publicizes monthly outbound spam volume and rankings for sample organizations in the treated group, including organizations in United States, Canada, Belgium, and Turkey. Daily spam data come from the Composite Blocking List (CBL) and the Passive Spam Block List (PSBL). The CBL gathers its source data from very large mail server installations and lists IPs exhibiting characteristics which are specific to open proxies of various sorts and dedicated Spam BOTs which have been abused to send spam, worms/viruses. The PSBL is an easy-on, easy-off blacklist that does not rely on testing and has lower probability of false positives because any user can remove their ISP's mail server from the list. The raw data include observed spamming IP addresses, corresponding outbound spam volume, and botnet tags in the forms of text files from CBL and Network News Transfer Protocol (NNTP) messages from PSBL. One important step in data processing is mapping IP addresses to netblocks and, subsequently, Autonomous Systems (ASs), which are groups of IP addresses owned by an organization. An AS can be identified by a unique Autonomous System Number (ASN). Only a few organizations in our data have multiple ASs. To avoid bias towards large organizations who own multiple ASs, we aggregate the data to the ASN level instead of organization level. Lastly, we aggregate the daily outbound spam data into monthly data and derive rankings for each country.



January 2012 Monthly United States ∇ All Sp@mRankings.net from CBL Volume

(Previous Month, Next Month)

Impressive churn! Comcast took three places in January, spewing almost 29% of the U.S. top ten spam, or more than GBLX and Charter's AS 20115 put together.

Rank (Previous)	Organization	Volume
1 (8)	Global Crossing Ltd. www.globalcrossing.com/ AS 3549 GBLX	1,214,235 13.7%
2 (5)	Charter Communications www.charter.com AS 20115 CHARTER-NET-HKY-NC	1,068,667 12%
3 (4)	Comcast Cable Communications Inc. www.comcast.com/ AS 33287 COMCAST-33287	1,011,895 11.4%
4 (3)	Server Central Network www.servercentral.com/ AS 23352 SERVERCENTRAL	893,625 10.1%
5 (-)	Access Integrated Technologies Inc. ezzi.net AS 15149 EZZI-101-BGP	879,664 9.91%
6 (6)	Comcast Cable Communications Holdings Inc www.comcast.com/ AS 7725 COMCAST-7725	793,319 8.94%
7 (-)	FDCservers.net fdcservers.net/ AS 30058 FDCSERVERS	792,398 8.93%
8 (7)	Comcast Cable Communications Holdings Inc www.comcast.com/ AS 20214 COMCAST-20214	762,175 8.59%
9 (-)	Network Operations Center Inc. www.nocinc.com/ AS 21788 NOC	754,454 8.5%
10 (-)	CDM www.primary.net/ AS 6428 CDM	704,073 7.93%

Comcast, Comcast, Comcast.

Figure 1. Screenshot of SpamRankings.net

The data processing is an issue surrounding the concept of “big data”. We receive more than 8 million records a day from CBL and others more from PSBL, which we automatically summarize into about 2 million spam messages observed from IP addresses worldwide. On the ASN level, we have seen 27,500 ASNs with spam volume over the lifespan of this project. The ASNs are then grouped and ranked by country. Only top 10 organizations with the largest outbound spam volume are presented on SpamRankings.net (Figure 1). In each ranking list, for each ASN, we publicize the following information: rank, rank in the previous month if it was listed as a top 10 spammer in the previous month, organization information including the name and website of the company, ASN, and outbound spam volume.

Quasi-Experimental Study

In our study, the organizations are clustered by countries. The outcome evaluations are based on comparing organizations in the treatment countries to organizations in other similar countries. For the purpose of this study, organizations within one country need to be ranked together. So we could not do random treatment selection at the ASN level. Therefore, we nest ASNs within countries and assign countries as clusters to the treatment conditions. As aforementioned, considering the authors’ PR connections to draw attention to disclosed information, we chose the United States, Canada, Belgium, and Turkey as four treatment countries. Based on the spam data from the CBL and the population data, we identified four countries with similar population and outbound spam volume to the treatment countries as shown in Table 1. Therefore, the comparison countries are Indonesia, Malaysia, Netherland, and Iran.

For the treated group, we publicized the spam rankings through SpamRankings.net monthly from May 2011 to January 2012. We treated different countries with differing starting points in time, with the United States in May 2011, Canada in June 2011, Belgium and Turkey in July 2011. This sequential release was designed to accumulate publicity for our ranking site before getting into the full-scale experiment. For the control group, we did not publish any information on outbound spam, but the same data were still collected of organizations in these countries and kept internally. We also collected static information on each AS, including number of IP addresses, number of unique IP addresses, number of prefixes, number of regions, network name, website, network type, traffic level, inbound vs. outbound traffic ratio, and geographic scope.

Table 1. Country Pairs

Pair	Country	Population	Spam*	Group
1	United States (US)	310,232,863	57,176,031	treated
	Indonesia (ID)	242,968,342	94,435,116	control
2	Canada (CA)	33,679,000	4,387,388	treated
	Malaysia (MY)	28,274,729	6,695,830	control
3	Belgium (BE)	10,403,000	3,781,796	treated
	Netherland (NL)	16,645,000	6,283,101	control
4	Turkey (TR)	77,804,122	14,759,146	treated
	Iran (IR)	76,923,300	13,291,908	control

* All the data on spam in this paper refer to the data on outbound spam
Spam data are taken from data for April 2011.

Since we want to engage both organizations and consumers and observe their natural reactions, it is necessary to maintain the exposure and publicity of Spamrankings.net. We promoted the website through different channels, including social media such as YouTube, Twitter, and blogs, conferences, and press releases, to increase the impact of SpamRankings.net. We also received many feedbacks from industries and observed that some organizations have already tried to take their names off the list on SpamRankings.net. For example, we received the following comment from a Chief Security Officer of a medical center, which also confirms that some outgoing spam could be reduced using basic controls.

"The first time we were rated #1 on your list, we noticed that one of our users had generated thousands of spam messages and asked her to change her password—that stopped the spam immediately. The next month, we found another user who had just given up her credentials and got her to change her password as well. I spoke with a colleague at one of the other medical centers ranked on your site and he mentioned they have the same problem…The listing on your site added additional impetus to make sure we 'stay clean' so in that regard, you are successful."

Data

We collected outbound spam data on the top 250 most spamming ASNs each month from March 2011 to January 2012 for the eight selected countries. Table 2 shows the summary statistics of observed sample ASNs by country. Only the United States had over 250 spammers for some months, but the top 250 ASNs account for over 95% of the total outbound spam. The total unique sample size is 1718 ASNs, with 1177 ASNs in the treated group and 541 ASNs in the control group. However, if we look at the average number of ASNs with observed outgoing spam per month, we have more balanced treatment group and control group. The unbalance is due to the observation that spamming ASNs for the treatment group varied significant from month to month, indicating that ASNs in the treatment group reduced their outbound spam more quickly than those in the control group. Results for average maximum of spam percentage by ASN show that a few ASNs were responsible for most outbound spam volume in Indonesia, Turkey, Belgium, and Malaysia. Especially for Indonesia, the most spamming ASN sent out 83.46% of total spam on average. However, for the United States, the most spamming ASN only accounted for 6.89% of total spam on average.

Table 2. Observed Sample ASNs by Country

	Number of ASNs	Average number of ASNs with positive spam volume per month	Average max of spam volume by ASN	Average max of spam percentage by ASN
Treated				
US	699	250	3,414,080	6.89%
CA	316	175	1,261,576	20.94%
BE	56	31	1,116,462	44.70%
TR	106	63	5,051,160	48.08%
Sum	**1177**	**519**		
Control				
ID	229	190	45,903,492	83.46%
MY	57	44	1,958,958	43.11%
NL	170	101	1,067,763	22.91%
IR	85	77	2,575,711	27.89%
Sum	**541**	**413**		

Table 3 summarizes the outbound spam volume by country for both the periods before (Pretest Period) and during (Test Period) the experiment. This comparison presents the average outbound spam volume per month and the difference. On average, the outbound spam volume of the four countries in the treated group dropped by 54.93%, while the number for the four countries in the control group is 45.84%.

Table 3. Outgoing Spam Volume Observed Per Month Per Country

	Pretest Period*	Test Period*	Difference	Percentage
Treated group				
US	105,347,424	33,007,389	72,340,035	68.67%
CA	7,786,736	3,949,362	3,837,374	49.28%
BE	3,812,537	1,663,925	2,148,612	56.36%
TR	14,758,174	8,052,961	6,705,213	45.43%
Average	**32,926,218**	**11,668,409**	**21,257,809**	**54.93%**
Control group				
ID	93,416,115	46,320,078	47,096,037	50.42%
MY	6,361,998	3,684,334	2,677,663	42.09%
NL	7,261,624	2,086,952	5,174,672	71.26%
IR	10,590,092	8,515,070	2,075,021	19.59%
Average	**29,407,457**	**15,151,609**	**14,255,848**	**45.84%**

*For US, the pretest period is March, 2011 to April, 2011, the test period is May, 2011 to January, 2012.
For CA, the pretest period is March, 2011 to May, 2011, the test period is June, 2011 to January, 2012.
For all other countries, the pretest period is March, 2011 to June, 2011, the test period is July, 2011 to January, 2012.

Statistical Models

We estimate a linear model to test the effect of security information disclosure. First, we employ a simple difference specification to directly compare the treatment and control groups:

$$Y_{ict} = \theta_0 + \theta_1 D_c + \varepsilon_{ict} \ , \qquad (1)$$

where the dependent variable Y_{ict} is the outcome of interest for AS *i* in country *c* at time *t*; and D_c is an treatment indicator variable for whether country *c* received security information disclosure. Hence, the estimate of the coefficient θ_1 indicates the difference between treatment and control countries. We utilize this model to compare baseline differences in pre-treatment conditions and to test the effect of spam information disclosure on firms' outbound spam.

Since the assignment of countries to treatment and control groups is not random in this study, the outbound spam is likely to be affected by pre-treatment conditions. It is thus necessary to include observable AS characteristics and baseline spam volumes as control variables in equation (1) to improve the precision of the estimated treatment effect. Therefore, we also run the following specification:

$$Y_{ict} = \theta_0 + \theta_1 D_c + \theta_2 X_{ic} + \omega_p + \varepsilon_{ict} \ , \qquad (2)$$

Where Y_{ict} and D_c are defined as in equation (1), and X_{ic} is a vector of pre-treatment AS characteristics including baseline spam volume and number of IP addresses. Since the assignment to treatment and control groups was stratified within country pairs (Table 1), we also include country pair fixed effects, ω_p, in equation (2).

Finally, we examine if the treatment effect interacts with baseline AS characteristics by running the following difference in differences model:

$$Y_{ict} = \theta_0 + \theta_1 D_c + \theta_2 X_{ic} + \theta_3 D_c * X_{ic} + \omega_p + \varepsilon_{ict} \ , \qquad (3)$$

where the interactive term $D_c * X_{ic}$ is added based on equation (2). The estimate of θ_3 captures the part of treatment effect moderated by baseline AS characteristics.

Because outbound spam may be correlated within country as a result of common policies and regulations, failure to correct the standard errors could result in an overestimate of the treatment effects (Bertrand et al., 2004). We therefore cluster the standard errors at the country level (the level of treatment assignment) in all of the above models. Cluster-robust standard errors permit heteroskedasticity and within-cluster error correlation, but can still over-reject with few (five to thirty) clusters (Cameron et al., 2008). We further use wild cluster bootstrap-t procedure to test the estimate of θ_2 in our main models (equation (2)) (Cameron et al., 2008).

Baseline Comparison

Because assigning firms into treatment and control groups are not random, it is necessary to test the difference in pre-treatment conditions that may be correlated with the outbound spam. If the difference is not statistically significant, then any differences in post-intervention outcomes between the two groups can be causally attributed to the intervention. Otherwise, pre-treatment difference needs to be controlled for to make precise estimation on treatment effect. To check if firm characteristics were similar or not between the two groups, we run regressions of the number of IP addresses and pre-treatment baseline spam volume (average spam volume for March and April 2012) on treatment status respectively using equation (1).

We present the comparison of firms at baseline in Table 4. Column 1 contains the average characteristics for the control group. Columns 2 and 3 present the estimated differences between the treatment and control groups. The results in column 2 do not include any controls, while those in column 3 control for country pair fixed effects. The differences in average baseline spam and IP number are statistically significant and large in magnitude. Specifically, the organizations in the treatment group generated about 50% less spam than those in the control group before the treatment. On average, the organizations in the treatment group also have about four times more IP addresses than those in the control group. Both two variables are likely to be correlated with post treatment outbound spam.

Table 4. Baseline Comparison

Dependent variable	Control Mean (1)	Treatment Difference No Controls (2)	Treatment Difference Country Pair FE (3)
Baseline spam	218439	-106540 (111622)	-152449** (57470)
IP number	140495	647773* (327720)	625859* (277616)
Observations	540	1717	1717

Note: Column 1 contains the average characteristic of the organizations in the control countries. Columns 2 and 3 contain estimates of the average difference in characteristics between the control and treatment organizations, without controls and with controls for country pair fixed effects, respectively. Standard errors are clustered by country and shown in parentheses. * indicates statistical significance at the 10% level, ** at the 5% level, and *** at the 1% level.

Results

The estimation of the effect of information disclosure is based on comparing the outgoing spam volumes of the treatment group and the control group, according to equation (1) and (2). The results are presented in Table 5. Column (1) displays the results from the basic model in equation (1) where only treatment indicator is included. It shows that although the treatment organizations sent out less spam than the control organizations, the difference is statistically insignificant. However, once we control for country pair fixed effect, the difference becomes significant and also increases in magnitude (Column (2)).

As suggested by Table 1, the treatment organizations significantly differ from the control organizations in terms of baseline spam and number of IP addresses. Therefore, in addition to country pair fixed effect, Column 3 also controls for baseline spam volume and number of IP addresses and serves as the main results of this study. It is not surprising that both baseline spam volume and number of IP addresses significantly affect post treatment outbound spam. Baseline spam volume is positively correlated with spam volume during the treatment period, indicating the persistence of certain security vulnerabilities. Unless the subject organization takes efforts to deal with these vulnerabilities, they will be continuously exploited by malicious attackers. Number of IP addresses is found to be negatively correlated with outgoing spam volume, suggesting that large systems tend to have less vulnerability. On the one hand, large systems provide attackers with more opportunities. On the other hand, large systems are likely to invest more in Internet security. Our finding suggests that the later force dominates the former one.

Controlling for baseline spam and number of IP addresses drops the estimate of the treatment effect by approximately 80% from 103197 to 17757, suggesting that the baseline spam and number of IP addresses explain a substantial part of variation in post treatment outbound spam. Nevertheless, the treatment effect remains significant and sizable even with controls for the two characteristics. Given that the average outgoing spam volume for the treatment group is 111,899, the effect size is estimated at approximately 15.9 percent. Romanosky et al. (2011) found that adoption of data breach disclosure laws can reduce identity theft caused by data breaches, on average, by 6.1 percent. While the two findings are consistent, the comparison suggests that public information disclosure can generate more effective results than notifying only those who have been affected.

Considering the small number of clusters, we use wild cluster bootstrap-t procedure suggested by Cameron et al. (2008) to further test the treatment effect estimate. The bootstrap result shows that the estimate is robust to such asymptotic refinement. In addition, to test if the estimate is subject to the functional specification of the statistical model, we take log transformation of spam volume, which smooths out the skewness in the distribution of spam, and run the same estimation again. According to the results presented in column (4), the treatment effect becomes even more significant statistically. Therefore, we can safely arrive at the conclusion that public disclosure of outbound spam does help reduce outbound spam.

Table 5. Effect of Information Disclosure

Dependent Variable	Spam	Spam	Spam	Ln(Spam)
Independent Variable	(1) Basic model	(2) Basic model +Country pair FE	(3) Basic model + Country pair FE +Controls	(4) Basic model + Country pair FE +Controls
Constant	121248* (52992)	163213*** (31879)	-1274 (4250)	6.4448*** (0.3441)
Treatment	-81393 (53820)	-103197** (30849)	-17757** (4076)	-2.8197*** (0.3669)
Baseline spam			0.4922*** (0.0160)	0.0000003 (0.0000002)
IP number			-0.0058*** (0.0005)	0.0000002*** (0.00000002)
Significance level using wild bootstrap-t			0.002	0.002
Observations	14255	14255	14248	14248

Note: Column 1 displays the estimate of treatment effect on outgoing spam using the basic model only including treatment indicator (equation (1)). Column 2 reports an estimate of the treatment effect on outgoing spam controlling for country pair fixed effects. Column 3 reports the estimate of the treatment effect on outgoing spam controlling for country pair fixed effects, baseline spam volume, and the number of IP addresses. Column 4 reports the estimate of the treatment effect on log transformed outgoing spam controlling for country pair fixed effects, baseline spam volume, and the number of IP addresses. Standard errors are clustered by country and shown in parentheses. Row significance level using bootstrap-t reports the significance level for the estimate of treatment effect in Column 3. * indicates statistical significance at the 10% level, ** at the 5% level, and *** at the 1% level.

To examine how the treatment effect dynamically changes as the treatment proceeds, we run the estimation for each month of the treatment period separately, controlling for country pair fixed effects, baseline spam, and number of IP addresses. The results for all seven months of the treatment period are presented in Table 6. Throughout the entire period, the estimates of treatment effect are consistent and increase in magnitude, which provides additional support for our conclusion.

Table 6: Effect of Information Disclosure by Time

Months into treatment	1	2	3	4	5	6	7
Independent Variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Constant	7429 (6124)	-10282* (4505)	-9821 (5828)	-7308 (5405)	-2276 (8665)	-6402 (7918)	9327* (4323)
Treatment	-15476* (7296)	-10843* (5229)	-14734** (5925)	-26353*** (4257)	-36988** (9620)	-18685 (12003)	-13304** (4541)
Baseline spam	0.3049*** (0.0043)	0.5125*** (0.0140)	0.4725*** (0.0141)	0.5256*** (0.0160)	0.7260*** (0.0332)	0.7520*** (0.0342)	0.3799*** (0.0103)
IP number	0.0012 (0.0012)	-0.0036** (0.0008)	-0.0035** (0.0014)	-0.0045** (0.0019)	-0.0131** (0.0029)	-0.0149** (0.0032)	-0.0051*** (0.0006)
Observations	1717	1717	1717	1717	1717	1717	1717

Note: Columns 1 to 7 display the estimates for the first to seventh month after the treatment. Country pair fixed effects, baseline spam, and number of IP addresses are included in all estimations. Standard errors are clustered by country and shown in parentheses. * indicates statistical significance at the 10% level, ** at the 5% level, and *** at the 1% level.

Then we allow the treatment effect to interact with pre-treatment characteristics to see if the effect would differ on different organizations. Table 7 presents the results. Column (1) simply displays the main results from column 3 of Table 5 without any interaction as a benchmark for comparison. Column (2) and (3) present the results allowing the treatment effect to interact with baseline spam volume and number of IP addresses respectively. Column (4) presents the results allowing the treatment effect to interact with the baseline rank, which is the spam ranking among all organizations in the same country at the time one month before treatment. Column (5) presents the results allowing the treatment effect to interact with baseline top10, which is a binary indicator for whether the organization ranked top 10 among all organizations in the same country at one month before treatment. Country pair fixed effects, baseline spam, and number of IP addresses are included in all columns. According to these results, the treatment effect does not interact with pre-treatment characteristics expect for baseline spam volume. The significant negative coefficient (-0.2524) for D_c* Baseline spam shows that information disclosure is more effective on organizations with more baseline spam. Although we only listed the top twenty spamming organizations, organizations currently off the list were also encouraged to take effort to remain that way. However, when imposed to public disclosure, organizations with severe outgoing spam problem have stronger incentives to deal with the problem to reduce reputation loss. This could be partially due to the specific presentation we used in this study, that we disclose the worst behavior instead of advocating the best practice.

Table 7: Interaction Effect of Information Disclosure

Independent Variable	(1) No Interaction	(2) Interact with baseline	(3) Interact with IP number	(4) Interact with baseline rank	(5) Interact with baseline top10
Constant	-1274 (4250)	-1478 (2363)	-1746 (2945)	-49205* (23181)	-9727 (10995)
D_c	-17757** (4076)	10656 (9605)	-17091*** (2791)	-86068 (47539)	-4212 (13915)
Baseline spam	0.4922*** (0.0160)	0.5027*** (0.0006)	0.4919*** (0.0166)	0.4942*** (0.0133)	0.4944*** (0.0128)
IP number	-0.0058*** (0.0005)	-0.0002 (0.0007)	-0.0002 (0.0193)	-0.0036** (0.0014)	-0.0049*** (0.0007)
D_c* Baseline spam		-0.2524** (0.0776)			
D_c* IP number			-0.0057 (0.0191)		
Baseline rank				244.2** (89.05)	
D_c* Baseline rank				-336.6 (217.7)	
Baseline top10					7820 (90440)
D_c* Baseline top10					-294164 (294193)
Observations	14248	14248	14248	14248	14248

Note: Column 1 displays the main results without any interaction effect from column 3 of Table 5 as a benchmark. Columns 2 and 3 present the results allowing the treatment effect to interact with baseline spam volume and number of IP addresses respectively. Column 4 presents the results allowing the treatment effect to interact with the baseline rank, which is the spam ranking among all organizations in the same country at one month before treatment. Column 5 presents the results allowing the treatment effect to interact with baseline top10, which is a binary indicator for whether the organization ranked top 10 among all organizations in the same country at one month before treatment. Country pair fixed effects, baseline spam, and number of IP addresses are included in all estimations. Standard errors are clustered by country and shown in parentheses. * indicates statistical significance at the 10% level, ** at the 5% level, and *** at the 1% level.

Conclusion

Governments, businesses, and consumers are constantly exposed to the risk of cyber attacks. Our society has recognized the need for additional laws and co-operation to protect consumer privacy, enterprise assets, intellectual property, and critical national infrastructure. In the thriving and fast moving discipline of Internet security, many are searching for technical solutions such as firewall and antivirus software. We propose that Internet security needs to be improved from the perspective of fundamental incentives. Systems are prone to failure when the person guarding them is not the person who suffers when they fail (Anderson and Moore 2006). An organization's security vulnerabilities are also suffered by other organizations but often kept private. Because of the lack of transparency and the existence of negative externality, organizations do not have enough incentive to adopt costly technical solutions.

In this study, we propose information disclosure as a potential public policy to improve Internet security. The public information disclosure can help achieve transparency and internalize externalities for organizations to improve their security. More importantly, instead of simple disclosure, the security information needs to be aggregated and presented in a relative way so that organizations are compared directly. Such direct peer influence can enhance the impact of information disclosure because of organizations' concern for reputation. Using a field study on outbound spam for over 1500 organizations in eight countries, we were able to show that public security information disclosure indeed reduced the outgoing spam, by approximately 15.9 percent. Comparing this number to existing study (Romanosky et al. 2011) suggests that public information disclosure is more effective than notification of affected individuals in inducing desired pro-social behavior. We also find that, even though only top spammers are disclosed, the information disclosure doses up all organizations within the range of disclosure. However, the impact is stronger on organizations with more spam, confirming that these organizations are subject to more reputation loss.

Our paper is the first to use security vulnerabilities data and provide implications for public policy evaluations. In this study, we collected data on outbound spam, one typical symptom for poor Internet security. For other security problems, data can be gathered through public policies that require mandatory reporting from each organization. It has been recognized that a key factor required for improving Internet security is the gathering, analysis, and sharing of information on security related problems. Our paper provides specific and feasible guidance toward such a direction. Public policy should not only consider information disclosure but also the way the information is presented to the public. For policy evaluation, more information presentation methods can be considered and compared before carrying out the policy extensively. The approach and implications apply to other social problems such as environmental issues like energy saving, pollution, carbon dioxide emission, etc., where the fundamental problem is the lack of incentive and the existence of negative externality. Information can be gathered and disclosed to build a reputation system, where reputation concerns can provide additional incentive and internalize externalities to encourage socially desirable behavior.

This paper is only our first step in studying Internet security and relevant public policy issues. We are planning to further extend the current study in several dimensions. First, we only experimented with ranking information in the current study. To identify the exact effect of using ranking information versus using absolute volume information, a new treated group can be added where organizations only receive information on absolute outbound spam volume with organizations listed alphabetically. Second, the observation of reduction in outgoing spam may or may not reflect the improvement in overall Internet security. If overall Internet security improves while spam decreases, it indicates that companies take the initiative to improve their overall infosec, affecting both vulnerability to spam and other threats such as phishing. This would mean that broad improvements in infosec can be achieved by presenting public information on certain security issues. It is also possible that in response to public information disclosure of outbound spam, organizations may take effort to address only outbound spam issue but still ignore other security problems. If this happens, it means that companies instead need to be individually incentivized to make improvements on individual dimensions of security. As a result, we can encourage companies to make improvements on spam by releasing information on spam, but to encourage companies to improve phishing, we need to also release phishing information. We can distinguish these two possibilities using information on other threats such as phishing. Last but not the least, we can drilldown outbound spam to botnets or snowshoe spammers to consider attackers' reactions to information disclosure.

Acknowledgements

The rankings and SpamRankings.net were produced in a research project funded by the National Science Foundation Grant No. 0831338. We would like to thank NSF for the financial support. We are also indebted to CBL and Team Cymru for providing us the raw data on outgoing spam.

References

Ackoff, R. L. 1961. "Management Misinformation Systems," Management Science (14:4), pp. 147-156.

Anderson, R. 2001. "Why Information Security is Hard: An Economic Perspective," in Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC), New Orleans, LA, December 10-14.

Anderson, R., and Moore, T. 2006. "The Economics of Information Security," Science (27:314), pp. 610-613.

Arora, A., Krishnan, R., Nandkumar, A., Telang, R., and Yang, Y. 2004a. "Impact of Vulnerability Disclosure and Patch Availability: An Empirical Analysis," Working paper.

Arora, A., Telang, R., and Xu, H., 2004b. "Timing Disclosure of Software Vulnerability for Optimal Social Welfare," in Proceedings of the Third Workshop of Economic Information Systems, Minneapolis, 1–47.

Benbasat, I., and Zmud, R. W. 2003. "The Identity Crisis within the IS Discipline: Defining and Communicating the Discipline's Core Properties," MIS Quarterly (27:2), pp. 183-194.

Bertrand, M., Duflo, E., and Mullainathan, S. 2004. "How Much Should We Trust Differences-in-Differences Estimates?" The Quarterly Journal of Economics (119:1), pp. 249-275.

Bonini, C. P. 1963. Simulation of Information and Decision Systems in the Firm, Englewood Cliffs, NJ: Prentice-Hall.

Broadbent, M., Weill, P., O'Brien, T., and Neo, B. S. 1996. "Firm Context and Patterns of IT Infrastructure Capability," in Proceedings of the 14th International Conference on Information Systems, J. I. DeGross, S. Jarvenpaa, and A. Srinivasan (eds.), Cleveland, OH, pp. 174-194.

Cain, D.M., Loewenstein, G., Moore, D.A. 2005. "The Dirt of Coming Clean: Perverse Effects of Disclosing Conflicts of Interest," Journal of Legal Studies (34), pp. 1-25.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," Journal of Computer Security (11), pp. 431–448.

Cate, F. 2009. "Comparative Approaches to Security Breaches," Symposium on Security Breach Notification Six Years Later: Lessons Learned about Identity Theft and Directions for the Future, Berkeley Center for Law and Technology, Berkeley, CA.

Carroll, J. 2005. "The Blacksburgh Electronic Village: A Study in Community Computing," in Digitial Cities III: Information Technologies for Social Capital, P. van den Besselaar and S. Kiozumi (eds.), New York: Springer-Verlag, pp. 43-65.

Carver, C. A., Hill, J. M. D., Surdu, J. R., and Pooch, U.W. 2000. "An Intrusion Response Taxonomy and Its Role in Automatic Intrusion Response," in Proceedings of the first IEEE Workshop on Information Assurance and Security, Los Alamitos, CA: IEEE Computer Society, pp. 129–135.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research (20:1), pp. 79-98.

Dillenberger D., and Sadowski, P. 2012. "Ashamed to be selfish," Theoretical Economics, (7:1), pp. 99-124.

Duflo, E., Dupas, P., and Kremer, M. 2011. "Peer Effects, Teacher Incentives, and the Impact of Tracking: Evidence from a Randomized Evaluation in Kenya," American Economic Review, (101:5), pp. 1739-1774.

Elias, L. 2001. "Full Disclosure is a Necessary Evil," SecurityFocus.com, www.securityfocus.com/news/238.

Farrow, R. 2000. "The Pros and Cons of Posting Vulnerability," The Network Magazine, www.networkmagazine.com/shared/article.

Festinger, L. 1954. "A Theory of Social Comparison Processes," Human Relations, (7), pp. 117 -140.

Forcht, K. A. 1994. Computer Security Management. Boyd & Fraser, Danvers, MA.

Frei, S., 2010. "The Security of End-user Pcs: an Empirical Analysis," in DDCSW: Collaborative Data-Driven Security for High Performance Networks, Internet2 and WUSTL, August.

Fung, A., Graham, M., and Weil, D. 2007. "Full Disclosure: The Perils of and Promise of Transparency," Cambridge, MA: Cambridge University Press.

Gal-Or, E., and Ghose, A. 2005. "The Economic Incentives for Sharing Security Information," Information Systems Research (16:2), pp. 186-208.

Gordon, L. A., Loeb, M., and Lucyshyn, W. 2003. "Sharing Information on Computer Systems Security: An Economic Analysis," Journal of Accounting Public Policy (22:6), pp. 461–485.

Hui, K.L., Teo, H.H., and Lee, S.Y.T. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," MIS Quarterly (31:1), pp. 19-33.

Jin, G. Z., and Leslie, P. 2003. "The Effect of Information on Product Quality: Evidence from Restaurant Hygiene Grade Cards," Quarterly Journal of Economics (118), pp. 409–451.

Kankanhalli, A., Teo, H.-H. Tan B. C. Y., and Wei, K.-K. 2003. "An Integrative Study of Information Systems Security Effectiveness," International Journal of Information Management, (23:2), pp. 139–154.

Kannan, K., Rees, J., and Sridhar, S. 2007. "Market Reactions to Information Security Breach Announcements: An Empirical Analysis," International Journal of Electronic Comerce (12:1), pp. 69-91.

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

Lenard, T.M., and Rubin, P.H. 2005. "Slow Down on Data Security Legislation," Progress Snapshot 1.9. Washington, DC: Progress & Freedom Foundation.

Lenard, T.M., and Rubin, P.H. 2006. "Much Ado about Notification," Regulation (29), pp. 44-50.

Luttmer, E. F. P. 2005. "Neighbors as Negatives: Relative Earnings and Wellbeing," The Quarterly Journal of Economics (120:3), pp. 963–1002

Mookerjee, V., Mookerjee, R., Bensoussan, A., and Yue, W.T. 2011. "When hackers talk: managing ifnroamtion security under variable attack rates and knowledge dissemination," Information Systems Research (22:3), pp. 606-623.

National Conference of State Legislatures (NCSL), 2012, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx.

Quarterman, J. S., Sayin, S., and Whinston, A. B. 2011. "Rustock Botnet and ASNs," in Research Conference on Communication, Information and Internet Policy (TPRC), Arlington, VA.

Quarterman, J. S., Whinston, A.B., Sayin, S., Kumar, E.V., Reinikainen, J., and Ahlroth, J. 2010. "Internet cloud layers for economic incentives for internet security", RIPE Labs, https://labs.ripe.net/Members/jsq/economic-incentives-for-internet-security.

Ponemon Institute. 2005. "National Survey on Data Security Breach Notification," Traverse City, MI: Author.

Ransbotham, S., and Mitra, S. 2009. "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," Information Systems Research (20:1), pp. 121-139.

Romanosky, S., Telang, R., and Acquisti, A. 2011. "Do Data Breach Disclosure Laws Reduce Identify Theft?" Journal of Policy Analysis and Management (30:2), pp. 256-286.

Saito, K. 2011. "Role Conflict and Choice: Shame, Temptation, and Justifications", Working paper.

Schneier, B. 2002. "Computer Security: It's the Economics, Stupid," Workshop on Economics and Information Security, University of California, Berkeley, CA.

Schwartz, P., and Janger, E. 2007. "Notification of Data Security Breaches," Michigan Law Review (105), pp. 913-984.

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

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

Toth, T., and Kruegel, C. 2002. "Evaluating the Impact of Automated Intrusion Response Mechanisms," in Proceedings of the Eighteenth Annual Computer Security Applications Conference, Los Alamitos, CA: IEEE Computer Society, pp. 301–310.

Yue, W., and Cakanyildirim, M. 2007. "Intrusion Prevention in Information Systems: Reactive and Proactive Response," Journal of Management Information Systems (24:1), pp. 329–353.