Cybersecurity Policies Design and Evaluation: Evidence from a Large-Scale Randomized Field Experiment*

Shu He
Department of Economics
The University of Texas at Austin
shuhe@utexas.edu

Gene Moo Lee
Department of Computer Science
The University of Texas at Austin
gene@cs.utexas.edu

John S. Quarterman
Quarterman Creations
antispam@quarterman.com

Andrew B. Whinston
Department of Information, Risk, & Operations Management
The University of Texas at Austin
abw@uts.cc.uexas.edu

*All authors contribute equally. This research is funded by National Science Foundation under the contract number 1228990. We thank Yun-sik Choi, Ying-Yu Chen, Mark Varga, Zeyuan Zhu, Niyati Parameswaran from the University of Texas at Austin and Markus Iivonen from the Helsinki Metropolia University of Applied Science for technical support. We are very grateful for the comments on the web design shared by Sarah R. Benoist, Meredith Bethune from the University of Texas at Austin and Ping Zhang from the Syracuse University, as well as the comments on statistical analysis shared by Dylan Walker from Boston University, Jason Abrevaya, Brendan Kline, Haiqing Xu from University of Texas at Austin. We are responsible for all the possible problems in the paper.

Abstract

Internet insecurity is now a serious threat to the world which attracted large attention from researchers and governments. In the present study, we propose a design of an independent security evaluation institution along with regulations on security information disclosure in order to effectively resolve cybersecurity problems. Specifically, we apply a large-scale randomized field experiment involving 7,919 U.S. organizations to evaluate the effectiveness of the target institution. We use outbound spam volume to estimate latent organizational security levels, then construct peer rankings to compare security levels among organizations in the same industry sectors. With the data collected from our experiment, we find evidence that the security information sharing combined with publicity treatment has significant effect on the spam reduction for large spammers. Moreover, we observe significant peer effect among organizations in the same industry sector after the experiment, and the peer effect is stronger among organizations in two treatment groups. Our design can be further implemented in extended experiments with organizations from other countries and more robust security indicator.

Keywords: Internet security, policy design, randomized field experiments, peer effect, spam

1 Introduction

> "Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas."
>
> – Barack Obama

In recent years, inadequate cybersecurity has become a serious threat to the world. Data shows that the average cost of security compromises may be as much as $3.5 million in 2013, which has increased 15% compared to the last year's data.[1] According to PWC's global state of information security report, the number of detected incidents has increased by 25% in 2013.[2] In addition, the popular book "*Spam Nation*" (Krebs, 2014) reported that anti-virus companies are fighting an average of 82,000 new attacks every day. McAfee had detected 14 million new pieces of malware in the first quarter of 2013 alone. One conspicuous example is Target Corporation's data breach, which affected 2.6 million consumers during the holiday season in 2013.[3] The incident caused a significant amount of business and reputation loss to the company and gave rise to wide public attention. Unfortunately, this is not the end of the tragedy. The emergence of endless sophisticated cyberattacks impulses us to find more efficient solutions to the problem.

The U.S. government has already taken measures to deal with the national security issues. The White House released the "*Cyberspace Policy Review*" in 2009 summarizing the near-term action plan for cybersecurity.[4] More recently, President Obama signed Executive Order 13636, "*Improving Critical Infrastructure Cybersecurity*," which emphasizes the importance of information sharing and cybersecurity framework development.[5] Similar cybersecurity regulation "*Article 13a*" has been implemented among member states of European Union. While these regulations show us the high-level directions to attack the problem, the details about implementation require further investigations. For instance, according to the Executive Order, the U.S. Department of Homeland Security will promote the adoption of cybersecurity framework through a voluntary program with the help of security experts from private sector. Given the fact that it is voluntary, the success

[1] Data source: 2014 Cost of Data Breach Study: Global Analysis by Ponemon Institute LLC.
[2] http://www.pwc.com/en_GX/gx/consulting-services/information-security-survey/assets/2013-giss-report.pdf.
[3] The data comes from the announcement of Target.
[4] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[5] http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636

of the program highly depends on how to incentivize organizations to participate in this program. For the security-related information disclosure part, the current convention is to passively publish security information in case of major incidents. Essentially, we lack an independent institution to monitor and evaluate the Internet security condition to prevent potential security attacks.

Researchers have investigated the root causes and countermeasures to mitigate the cybersecurity issues for a long time from technical and economic perspectives. Computer security researchers have developed various technical solutions to the cybersecurity issues including spam filtering (Sahami et al. 1998; Bratko et al. 2006; Cormack and Lynam 2007), intrusion detection systems (Denning 1987; Lee and Stolfo 1998; Roesch 1999), digital forensics (Casey 2011; Taylor et al. 2014), and so on.

Besides the technical approach, there is a large number of cybersecurity research projects based on economic theory. In this literature, the research community has come to a general consensus that cyber insecurity is partially due to underinvestment, which is the result of distorted incentives by asymmetric information, network externalities, and moral hazard (Anderson 2001; Bauer et al. 2009). Researchers also studied the behaviors of the attackers using observational data, hunting for the "bottleneck" of the criminal activities to solve the problem efficiently as in Levchenko et al. (2011), van Eeten et al. (2011), and Moore and Clayton (2011). Furthermore, other studies look at how users, companies, and software vendors' response to vulnerability disclosure or security information awareness, including Arora et al. (2004) and D'Arcy et al. (2009). An alternative solution is to improve the defender side: organizational level security protection. There are studies suggesting that ISPs are suitable to prevent malicious cyber behaviors as in Wood and Rowe (2011). However, unlike individual consumers, many organizations do not use service from ISPs. With rapid increase of data breaches in retails, financial services, and health service companies, it is very important for every organization to get enough protection against cyber attacks.

In our preliminary results in Quarterman et al. (2012), Qian et al. (2013) as well as Moore and Clayton (2011), we found evidence that security information publication helps improve Internet security condition on the country level. In the present paper, we want to take one step further to evaluate the effectiveness of spam information publication on organizations across different industry sectors. In this paper, we propose a design of an independent security evaluation institution along with regulations on proactive spam information disclosure to alleviate the Internet security problem.

The ultimate goal is to set up a nationwide institution sponsored by the government to monitor and evaluate all organizations' security conditions. Ideally, the institution will monitor all organizations' security performances such as spam, phishing and DNS attacks over time and publish them on its public website. Beneficial from the data, the institution can evaluate the latent security condition for each organization. In this way, the evaluation agency works the same as Moody's or S&P for bonds. The rationale behind this institution is as follows. First, the information disclosure helps the information asymmetry issue. Due to insufficient internal resources and policies, organizations may not have a full understanding of their security problems (D'Arcy et al. 2009). The proposed institution can alleviate this problem by providing complete, real time security information. Furthermore, our design contributes to the lack of motivation problem. Given the negative externality of information insecurity, organizations may not have strong incentives to actively prevent security breaches, especially when the cost of Internet security prevention is relatively high. Publicizing internet insecurity information applied pressure on firms to fear the loss of customers from their competitors (Gal-Or and Ghose 2005; Tang et al. 2013). Other related studies measured the impact of vulnerability information notification on remedies and countermeasures (Stone-Gross et al. 2009; Moore and Clayton 2011; Vasek and Moore 2012; Zakir et al. 2014; Rossow 2014). However, since those works are not based on rigorous randomization, it may be hard to claim causal effects of the notifications.

Randomized field experiment is regarded as the gold standard to estimate the counterfactual treatment effects of proposed policy. As an alternative to observational data analysis, randomized field experiment is regarded as a reliable empirical method to set causal treatment effect without confounding factors in a wide range of literature such as economics, marketing, information system, sociology, and other social sciences. As a result, it is commonly used in social science to evaluate the effectiveness of a proposed policy before its final implementation since it can help us to get the causal results of the policy intervention in vivo world with relatively low cost (Harrison and List 2004). However, as far as we know, it is rare for information system literature to take advantage of randomized filed experiment in policy development.

We conducted a large-scale randomized field experiment to evaluate the effectiveness of the proposed policy on organizations' Internet security conditions among 7,919 U.S. organizations. To estimate the latent security level of different organizations, we use outbound spam volume as the

main proxy for the underlying security condition to estimate the treatment effects since it is one of the security-related data sources which can be externally observed by outsiders (researchers) without any internal audits. To support the scale, we implemented a cloud-based treatment system, which can be used to conduct more experiments. With careful randomization design, we identify and distinguish the treatment effects of information awareness and publicity. Our results show that security information alone does not have significant influence, while the combination of information and publicity motivates large spammers to change their security strategies. Furthermore, with peer effect statistical analysis, we find evidence that organizations' security decision is influenced by average outcome of their peers, and the treatment effects are larger for the organizations in treatment groups. This interesting findings give us confidence that our unique "peer ranking" is effective in spam reduction. We also find that organizations' responses to our treatment vary according industry competitiveness.

Our study contributes to the literature by extending prior work on the effects of security information disclosure and by providing potential policies to mitigate the Internet insecurity problems. More importantly, our approach can be generalized and extended to other potential security remedies in different environments. As our current experimental universe only includes U.S. organizations, the conclusions in this paper may not be sufficiently applicable to organizations in other countries with different economic environments. Researchers and government staff in other countries can follow our large-scale field experiment supported by the cloud computing to design effective policies for their own countries. To build more robust organizational security metrics, we plan to incorporate multiple security-related data sources such as spam, phishing, and denial-of-service attacks. Lastly, with the constructed security metrics, we can potentially set up cybersecurity insurance premiums for cyber risks.

The remainder of the paper is organized as follows. Section 2 describes the experimental design and Section 3 provides the treatment system implementation, followed by the hypothesis development in Section 4. Section 5 describes our data and empirical analysis. Robustness check and discussions are presented in Section 6. Section 7 concludes the paper with future directions.

2 Experimental Design

The proposed third-party government sponsored institution could be quite costly considering the large number of existing organizations. Thus a preliminary evaluation of the design's effectiveness is prudent. We conducted a large-scale randomized field experiment from January 2014 to March 2014 on 7,919 U.S. organizations to see the treatment effect of information disclosure on spam volume reduction. To be more specific, we had three treatment groups with two different information disclosure methods to distinguish publicity effect from information awareness effect. The whole experiment can be summarized in Figure 1.

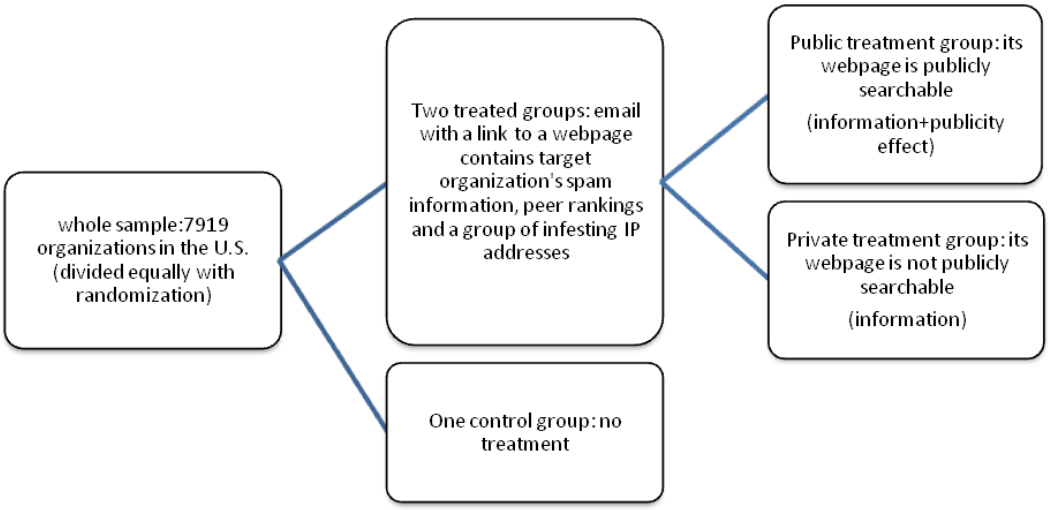


Figure 1: Design of the RFE

To measure latent Internet security conditions for each organization, we have to find a good proxy for them. Our approach is to use outbound email spam volume as a proxy of latent security levels. Spam volume is a good choice for the following reasons. As in Rao and Reiley (2012) and Moore and Clayton (2011), most outbound spam (over 90%) is sent from botnets which are the networks of virus-infected computers. Thus spam emission is an informative sign of underlying security issues. These compromised computers may also be used for even worse cyber criminal activities such as identity thefts, blackmails, and denial-of-service attacks. In addition, according to "*Spam Nation*", spam email is now the primary impetus for the bot herders to develop malicious software. Thus organizations with larger spam volume may have higher risk of data breach attacks. Another

important reason of the choice is that spam information is a reliable data externally observable without internal system audits. Compared with survey-based approach (D'Arcy et al. 2009), research using observational data can exclude the potential intrinsic data bias concern due to respondent dishonesty, a low response rate, and organizations' misunderstanding of their own situations.

To control for the heterogeneity of organizations, we divided all of the organizations into three equal-sized groups with a stratified, match-pair randomization.[6] The first group is the control group, which we do not apply any treatments on. For the two treatment groups, we sent treatment emails to relevant contacts in various departments (from marketing to IT) within each organization to inform them their security evaluation results at the end of January and March. Each treatment email included (1) organization's spam volume, (2) peer rankings, (3) spamming IP addresses, and (4) a link to a designated web page for the treated organization. The difference between the private and public treatment groups is whether the information of the focal organization is publicly searchable on our website. For the organizations in the public treatment group, the emails inform them that the spam information is publicized on our treatment website.[7] Conversely, the privately treated organizations are notified that the web page directed by the link in the email is not publicly available. With this setting, the difference of average spam volume between the control and the private treatment groups is due to the information awareness effect. Similarly, we can estimate the publicity treatment effect with the difference between the private and public treatment groups.

Peer ranking system based on the security level is another major contribution of the paper. Essentially, organizations within an industry sector are ranked according to their spam metrics. Sectors are defined by the two digits in two industry codes: Standard Industrial Classification (SIC) and North American Industry Classification System (NAICS). Note that high ranks indicate low security level, and that all of the organizations with no spam will be ranked equally with the lowest rank.

3 System Implementation

This section describes how the data is collected and processed, how the treatment system is implemented to support the large-scale experiment, and how the experiment team interacted with the

[6] The randomization detail is in the Appendix.

[7] Figure 8 in Section 3.3 shows a snapshot of our website.

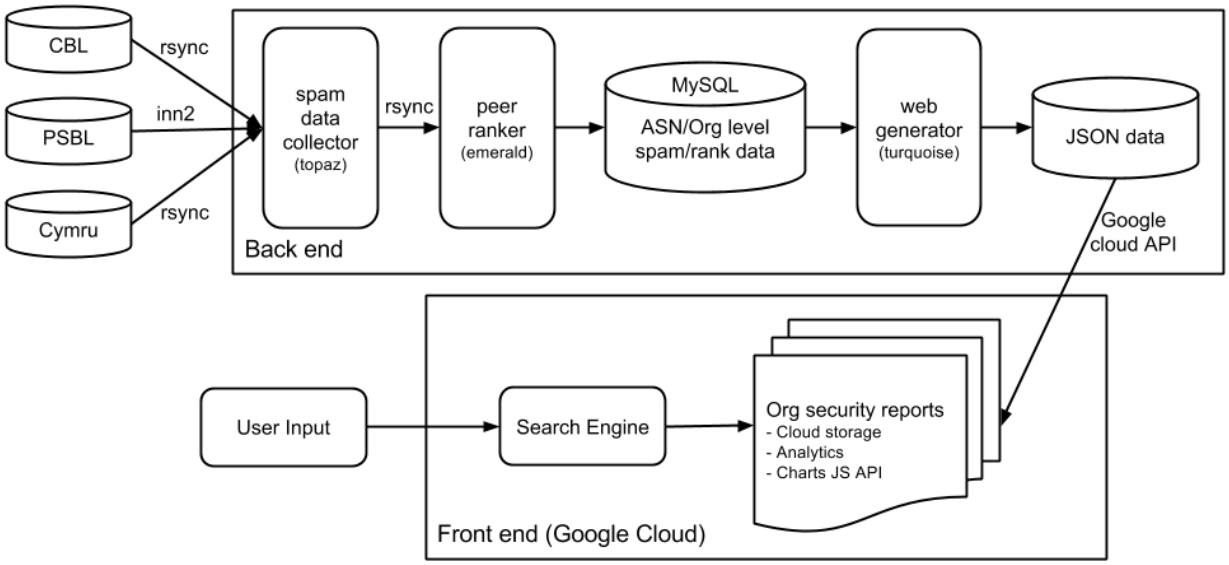


Figure 2: Treatment system design and implementation

treated organizations and the public. Figure 2 shows the architecture of the treatment system.

3.1 Data Collection

As discussed in Section 2, we use the outbound spam volume as the major indicator of organizations' latent security condition. We have collected daily feeds from spam blocklists. A spam blocklist is based on sampled data collected from spamtraps, which may have biases based on the settings of the spamtraps (Pitsillidis et al. 2012). Thus we use two independent spam feeds: Spamhaus' Composite Blocking List (CBL)[8] and Spamikaze's Passive Spam Block List (PSBL).[9] CBL daily aggregated reports are transferred to our back end system through `rsync`. On the other hand, PSBL provides a real-time news feed of the actual spam contents through InterNetNews (`inn`). Each blocklist provides daily reports on the list of spamming IP addresses and the total volume associated with each IP address. We term the total volume to be "Volume" and spamming IP count to be "Host." In summary, we have four data points: CBL Volume, CBL Host, PSBL Volume, and PSBL Host. CBL also provides the botnet associated with the spamming IP address.

To make sure our system correctly receives the daily feeds, we employ an email alerting system to report potential issues to the experiment team. Moreover, we developed a backup system to store raw data into multiple physical disk spaces for fault tolerance.

[8] http://cbl.abuseat.org/
[9] http://psbl.org/

One limitation of the spam feed data is related to network address translation (NAT). Due to the insufficient IP space, many organizations employ NAT to assign multiple hosts to a single IP address. Essentially, from the external observer's viewpoint, it is hard to distinguish the individual hosts behind a NAT box. In case of multiple infected hosts behind a NAT box, we only observe the frequently appearing botnet. Still, we emphasize that this NAT box issue does not affect the organizational security level evaluation because all the hosts behind NAT boxes do belong to the organization and the total spam volume is correctly reported.

From this raw IP-level data, we need to construct organization-level data to evaluate organization's security condition. To do that, we need three levels of mapping from IP to netblock, to autonomous system number (ASN), then finally to organization. The data is based on IPv4 address space, which uses classless inter-domain routing (CIDR).[10] Thus IP to netblock mappings, also known as IP lookup, is a longest prefix matching problem, which has a well-known efficient algorithm (Dharmapurikar et al. 2003). For netblock to ASN mappings, we receive daily netblock-ASN data feeds from Team Cymru through `rsync`.[11] In average, we have 584,000 netblocks and 49,000 ASNs in our mapping data. Lastly, for ASN to organization mappings, we group ASNs by the operating organization. Note that we only process ASN located in the U.S. for this experiment. For each ASN group, we then find the corresponding organization by searching the LexisNexis database.[12] As a result, 7,919 U.S. organizations are identified for the experiment.

One thing to note is that the Internet addressing system changes dynamically due to various organizational changes such as mergers and acquisitions, organizational structure changes, bankruptcy, and so on. Thus, in order to maintain an up-to-date Internet address mapping, we need to keep track of the changes on the autonomous system (AS) information. In case of AS title changes, we need an algorithmic way to identify the corresponding organizations. For this experiment, we use a string similarity matching algorithm (Dice 1945) to identify the changes of organizational governance on the Internet addressing space. For the treatment email correspondence, we use the email addresses obtained from the regional Internet registry (RIR) responsible for the U.S.: American Registry for Internet Numbers (ARIN).[13] The target institution we are proposing may need

[10] http://tools.ietf.org/html/rfc1519
[11] http://www.team-cymru.org
[12] http://www.lexisnexis.com
[13] https://www.arin.net/

to employ a reporting system from RIRs and organizations so that the security incidents can be properly associated to the correct organizations and the security evaluation reports can be delivered properly.

The aforementioned procedure to construct organizational spam data can be generally used, not limited to the U.S. ASNs. To conduct field experiments in other countries, the only additional tasks are to identify ASN groups and to extract email contact information from RIRs such as ARIN, APNIC, RIPE, and AfriNIC.

CBL data provides extensive view of the spammers' behavior covering more than 8 million IP addresses, 190,000 netblocks, 21,000 ASNs, and 200 countries. In the meantime, PSBL data size is an order of magnitude smaller than that of CBL. This is due to the difference in the number spamtraps each data feed uses. ASN and organizational spam data feeds are inserted into MySQL database.

3.2 Peer Ranking Construction

With the organizational spam information, the next step is to construct peer rankings to realize peer effects in the experiment. This is a major contribution of this paper, as other websites publishing spam information do not consider peer effects. Essentially, we need to rank organizations that fall into the same industry sector. We again use LexisNexis database to identify the industry codes – Standard Industrial Classification (SIC) and North American Industry Classification Code (NAICS) – for each organization in our experiment. We use the first two digits of the industry codes to group organizations, then rank them according to their spam metrics. In addition, we acquired industry concentration ratios data from U.S. census.[14]

Our main ranking is derived by a composite Borda count, as in Adelsman and Whinston (1997), from four constituent rankings with CBL Volume, CBL Host, PSBL Volume, and PSBL Host. A Borda count is a voting system that combines multiple orders of preference into a single composite metric. If an organization is ranked k, then it will get a point of $n - k$, where n is the number of total organizations in the ranking. The sum of these points is the Borda count for each organization. Organizations with higher Borda counts are ranked higher. Note that higher ranks indicate lower security levels and that all the organizations with no spam will be ranked equally with the lower

[14] https://www.census.gov/econ/concentration.html

rank.

To provide both macroscopic and microscopic views of the rankings, the treatment system calculates daily and monthly rankings. Monthly rankings are generated at the end of a month, while daily ones are calculated as we collect daily spam feeds. The target institution may face computational issues as the number of organizations is increasing and the number of observed spams can be intractable. For example, our peer ranking system produces 250,000 rank data records in a daily basis. The number will increase rapidly with more ranking criteria. Thus we argue that the spam collection and ranking construction should leverage parallelism such as MapReduce using the cloud computing platforms.

3.3 Treatment Channels: Email and Website

In our experimental design, we have two distinct treatment channels: email and website. For the private and public treatment groups, we sent treatment emails to deliver the organizational security reports. Each security report includes monthly spam-related records such as total volume, number of spamming IP addresses, peer rankings in the industry sector, and a list of spamming IP addresses if any. The spamming IP list provides a convenient way to isolate and mitigate the cyber risks in the organization. In order to make a distinction between the two treatments, private treatment emails make a clear statement that the report is exclusive to the organization and public treatment ones mention that the data is public in the website as shown in Figure 7. For the private treatment, we have instrumented a specialized URL parameter, which is only provided in the private emails. Lastly, to comply with CAN-SPAM Act, all our emails include a description on the purpose of the project and, for opt-out request, a postal address, telephone number, web form, and email address.

Besides the emails, we implemented a public website, `http://cloud.spamrankings.net`, to provide organizational security reports to the treated organizations and the public. To support a large-scale field experiment and eventually multiple experiments, the treatment website is constructed on a Google cloud platform. Cloud platform can efficiently scale to serve a large number of website visitors with an efficient content caching algorithms. We argue that other large-scale field experiments can also leverage cloud approach for scalability.

Each security report is a webpage that reads JSON files and produces visual graphs using Google

Charts JavaScript API.[15] Our back end produces JSON files that contain the data points for the monthly security evaluation reports. JSON files are transferred to the Google cloud storage using Google cloud API.[16] Then Google Charts API visualizes the JSON data in the web client. Figure 8 shows a screenshot of an organizational security evaluation report. The website contains similar content that the treatment email has: spam volume, spam host, peer rank, and industry codes. In addition, the website shows (1) daily spam metrics of the target organization, (2) ASN pie charts, and (3) botnet pie charts. Visitors can retrieve different reports based on data sources (composite Borda, CBL Volume, CBL Host, PSBL Volume, and PSBL Host), years, months, and classification methods (US, NAICS, and SIC).

The website are instrumented with Google Analytics for web traffic analytics.[17] Google Analytics JavaScript API keeps track of various features about the visitors such as geographic locations, service providers, web browsers, and so on. In order to measure the visitors due to our treatment emails, we use URL parameters that are uniquely assigned for each treatment email.

Our website implementation also supports the experimental design with two distinct treatment groups. For the public treatment, we develop a search engine that enables the general public to access the data on the public treated organizations. Visitors can search different organizations by names, AS numbers, websites, and industry codes. On the other hand, security reports on the private treatment group can only be accessed with the specialized URL parameters that were provided by the treatment emails.

3.4 Interaction with Treated Organizations and the Public

Peer effects will work better if our treatment websites gain visibility. We consult with the university's PR professionals to improve the engagement with the general public by producing an infographic and preparing press releases. Our blog,[18] Twitter,[19] and Facebook[20] pages are live and ramping up content, drawing both from external events and from interesting internal reports we observe.

Based on the Google Analytics report, the website had 2,370 unique visitors with 11,477 total

[15] https://developers.google.com/chart/
[16] https://cloud.google.com/storage/
[17] http://www.google.com/analytics/
[18] http://blog.spamrankings.net
[19] @spamrankings
[20] https://www.facebook.com/spamrankings

pageviews. In average, each visitor has spent three minutes in our website with 3.57 pageviews. Geographically, 64% of the total sessions are from the U.S., and other countries include Taiwan, Canada, Finland, and the Netherlands. 79% of the visitors are using English as their primary language. In terms of the traffic sources, a majority of the visitors (79%) came to our website via direct links, meaning that they have clicked the links provided in the treatment emails. More than 90% of the visitors used desktops to view the website.

4 Hypothesis Development

This paper proposes an information sharing policy of Internet security, which does not exist in the current world, and builds up a large-scale randomized field experiment to counterfactually test the results of the policy. If our proposed policy interference is effective, then organizations in the treatment groups will have less spam volume compared those in the control group after our treatments.

4.1 Information Disclosure Effect

Information disclosure effect refers to the treatment effect of spam information provided in our treatment emails on organizations who neglected the importance or did not have a full understanding of the security conditions due to lack of sufficient internal resources and policies (D'Arcy et al. 2009). The detailed spam information includes spam volume, number of spamming hosts, specific infesting IP addresses, compositions of spam volume over time as well as its relative performance compared to close competitors within the same industry. After receiving our emails, organizations without good knowledge of their security levels fully realize their own situations. In addition, they also get information that helps them to quickly resolve the problems. If our email treatment with security information is effective, we expect the spam volume of organizations in the private treatment group, who only receive emails from us, will decrease compared to that in the control group. Hence, we hypothesize:

Hypothesis 1 *There will be a significant decrease of spam volume after the experiment for organizations in the private treatment group compared to those in the control group due to the spam information disclosure in the email treatment.*

4.2 Publicity Effect

Publicity effect refers to the treatment effect on the public treatment group by publishing spam information and relative performance of organizations on our public website. Due to information asymmetry, it is difficult for customers and investors to get relevant security information for organizations when they make decisions on information sharing or investments. Given the negative externality of information insecurity, organizations lack motivations to make significant investment on Internet security, especially when the cost of Internet security improvement is relatively higher than the potential cost of data breach. Security information publication can create pressure on firms of the loss of reputations and customers (Gal-Or and Ghose 2005; Tang et al. 2013), which further encourages those organizations to take more stringent measures on the security protection. If our publicity treatment is effective, we would expect to see further decrease of spam volume for the public treated organizations, who receive both emails and publicity treatment, compared to that of the private treated organizations. We therefore propose the following hypothesis:

Hypothesis 2 *There will be a significant decrease of spam volume after the experiment for organizations in the public treatment group compared to those in the private treatment group due to the spam information publicity treatment.*

In addition, it costs less for organizations with more spam volume to find and fix security problems. From reputational aspect, it may be much worse for one organization to be on the bottom of the spam performance ranking than it to be in the middle of it. So our potential policy interference may be more effective for organizations with larger spam volume:

Hypothesis 3 *Organizations in the public treatment group with more spam volume tend to have larger spam volume drops after the experiment.*

4.3 Industry Characteristics

In addition, organizations in different industrial environments may react to our treatments in different ways. The concentration ratio of each industry is an important factor for organizations to make business decisions. Generally, people will assume that organizations in more competitive industry will present larger treatment effect due to larger demand elasticity. However, organizations'

decisions on Internet security measures with respect to industrial competitiveness is not that easy to determine. With little information transparency, the private cost of high spam volume is quite ambiguous. Unless the weak security condition leads to serious data breach scandals, there is little private cost on organizations. The situation is more severe when the cost of improving the security system is substantial. In that case, organizations may prefer to invest the resource in other areas with more promising payoffs. So we hypothesize:

Hypothesis 4a *Organizations from more competitive industry tend to have larger treatment effects.*

Hypothesis 4b *Organizations from more competitive industry tend to have smaller treatment effects.*

4.4 Peer Effect

Peer effect refers to the change of an organizations' Internet security performance that is influenced by its peer organizations' performances. Theoretically, peer effect is driven by reputational concerns, observational learning, and other factors. For example, organizations in the same industry may have technical knowledge exchange among their employers. However, due to the information asymmetry of Internet security, there is no easy access to get transparent and reliable information considering of other competitors' Internet security information. Currently, there are only a handful of websites that publish spam information such as CBL, Spamhaus, and Cisco. These rankings only provide incomplete spam information of "top spammers." And most of their information is based on the unit of ASN rather than organization.[21] Furthermore, most companies are more likely to passively disclose only information security issues related with compromised customer information at present, which may lead to underestimated information risk. The information issue may make the peer effect less significant.

In our experiment, we emphasize the importance of peer effect in our treatment by providing peer rankings in addition to the general spam information such as the monthly spam volume. Since Festinger (1954), social psychology literature has extensively investigated the social comparison theory,

[21] Classic.SpamRankings.net presents the top 10 spammers per country (http://www.spamrankings.net/classic/). Spamhaus has top 10 spam producing countries, ISPs and spammers each day (http://www.spamhaus.org/statistics/countries/). Cisco, on the other hand, has at most top 100 spam senders by IP, network owners and country (http://www.senderbase.org/static/spam/).

which demonstrated how individuals' behavior is influenced by the comparison between themselves and others. Harper et al. (2010), through a field experiment, finds that people's movie rating decisions will be influenced by median user's behavior. In our experimental setup, organization and its customers can have a direct comparison with its close competitors with our industrial level spam rankings. Hence, organization may change their behaviors on their cybersecurity strategies in response to peer organizations' security performance. Moreover, since only organizations in the treatment group will receive our treatment emails, we expect that these organizations will display larger peer effect compared to those in the control group. So we hypothesize:

Hypothesis 5 *Organization's spam performance is influenced by their peers.*

Hypothesis 6 *Organizations in the treatment groups are subject to larger peer effect than those in the control group.*

5 Empirical Analysis

5.1 Summary Description

Changes in the outbound spam are the basis of our experiment, but spam volume fluctuates dramatically from month to month. While the most relevant reason of outbound spam volume changes is the change of organizational security levels, there could be other possible reasons such as the change of spam demand in the black market and botnets' strategic move from some IP addresses to others to avoid being detected. Thus, we use the average spam volume over multiple months in the statistical analysis. Data shows that more than half of the organizations with positive spam volume have experienced one or two spamming episodes a year. Thus we use the six-month average spam volume right before the experiment started as the pre-experimental spam volume. Since our experiment started at the end of January 2014, we regard the time frame between July 2013 and December 2013 to be the pre-experimental period and the one between February 2014 and July 2014 to be the post-experimental period.

We use the natural logarithm transform for the outcome variables (monthly spam volume and number of spamming IP addresses) and the covariate (number of IP addresses). This is because the distributions of spam volume, number of spamming IP addresses and number of total IP addresses

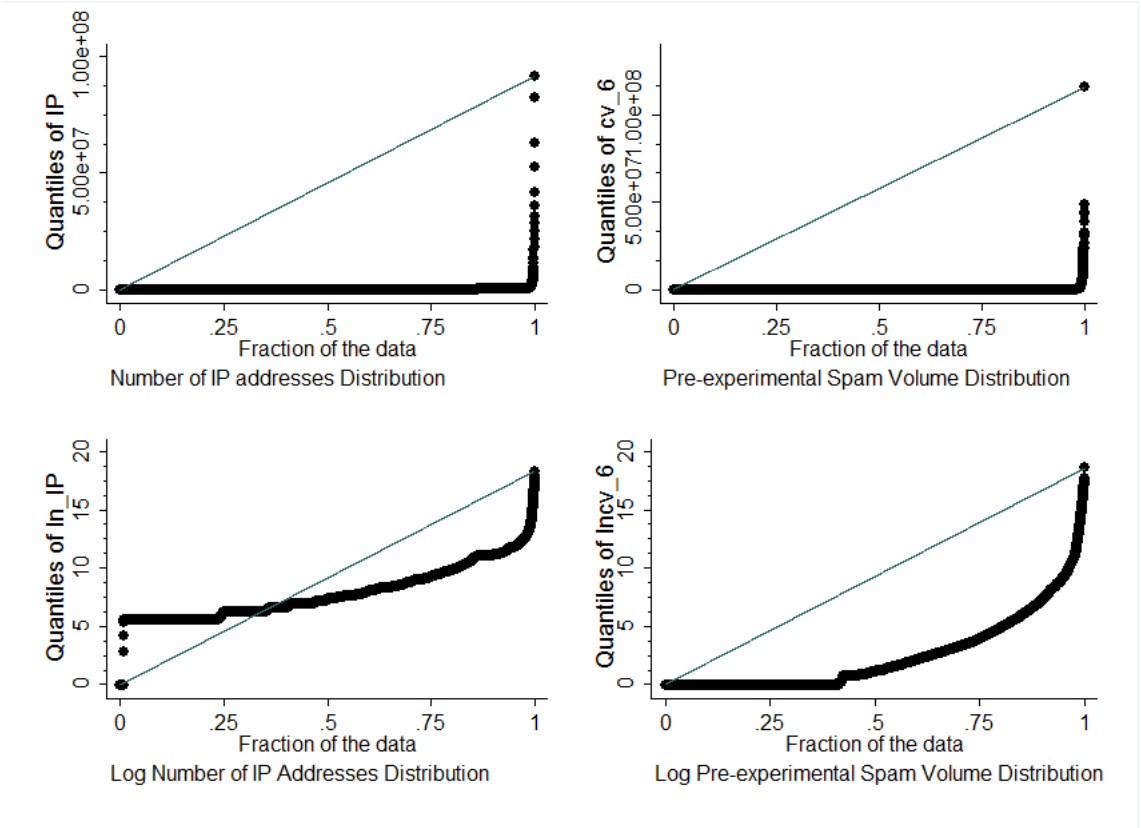


Figure 3: Distributions of spam volume and number IP addresses

are highly positively skewed as in Figure 3. The power of the experiment has significantly improved with the natural logarithm transform.

From the data, we observe that organizations' spam volume decrease on average after the experiment. It may be due to the rapid increase of data breach announcements at the end of 2013. This had attracted a lot attentions from the public, so organizations generally became more cautious about their security. In addition, the difference between spam volume before and after the experiment is quite heterogenous among organizations. From Figure 4, we can see that organizations with zero or small initial spam volume were worse after the experiment started, while top 25% spammers' outbound spam volume has decreased. It may be due to the fact that mall spammers, especially the organizations with zero spam volume, could hardly improve their security condition any more. On the other hand, organizations in the treatment groups with large number of spam volume will face the risk of losing customers and investors with our experiment, leading to more cautious strategies on their security protection. We also observe that spam performance of organizations vary among

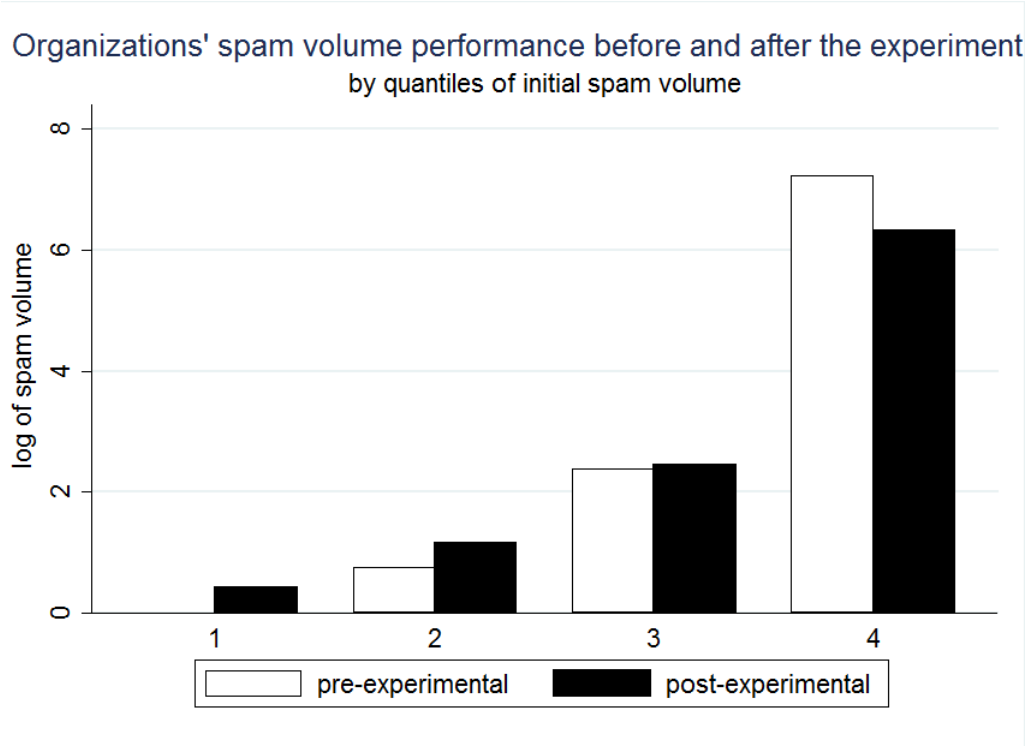


Figure 4: Spam performance within each quantiles for all organizations

different industry groups as shown in Figure 5. This can be explained by the distinct business models and characteristics of different industries.

The summary statistics of the related variables are listed in Table 1.

5.2 Internal Validity

The advantage of randomized field experiment is that the random assignment ensures the exogeneity of the treatments and the exclusion of selection bias (Duflo et al. 2008). In the randomization

Variable	Obs	Mean	s.d.	Min	Max
log (Post-experimental spam volume+1)	7,919	2.469	3.139	0	17.913
log (Number of post-experimental infested hosts+1)	7,919	1.830	2.072	0	12.134
log (Pre-experimental spam volume+1)	7,919	2.474	3.258	0	18.566
log (Number of pre-experimental infested hosts+1)	7,919	1.738	2.064	0	12.261
log (Number of IP addresses)	7,919	7.807	2.289	0	18.333
Number of infesting botnets	7,919	1.175	2.677	0	40.5
Publicly traded or not	7,919	0.0885	0.284	0	1
log (Number of employees)	7,021	1.410	0.605	0	2.860

Table 1: Summary statistics

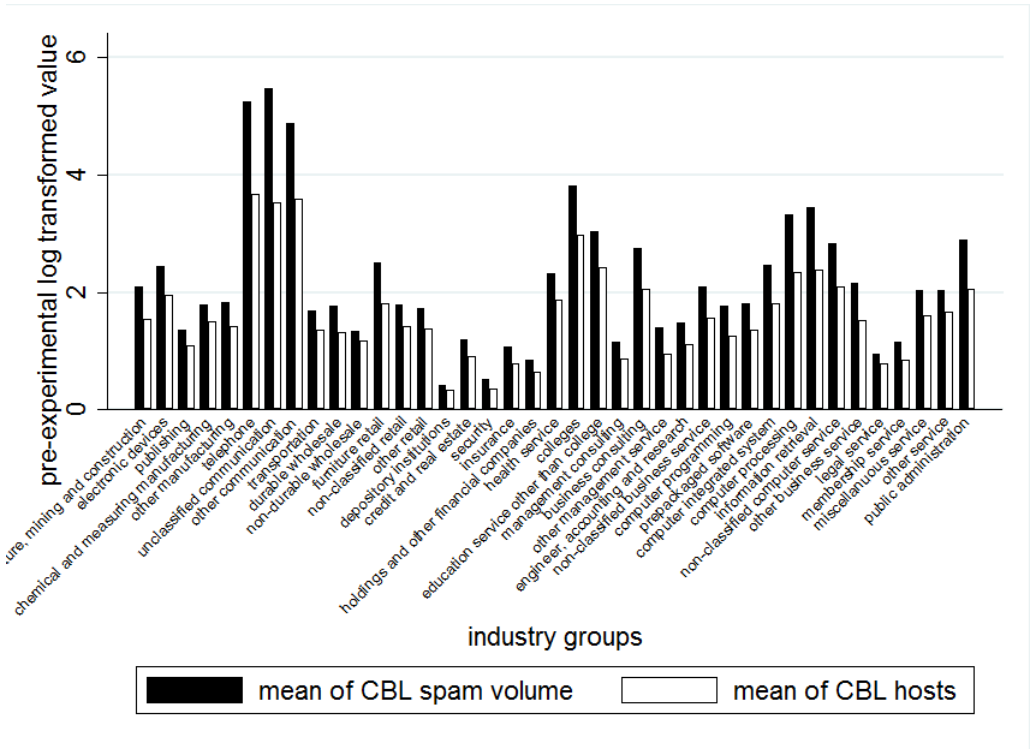


Figure 5: Spam performance in different industry groups

process, each organization has the same probability to be in one of the three groups, hence on average, organizations in the control and treated groups have homogeneous characteristics. However, it has been well known that a pure random assignment may have a probability of imbalance along some dimensions (Bruhn and McKenzie 2008). To ensure that any differences of post-experimental spam volume between the treatment and control groups can be causally attributed to the treatments, we have to verify the exogeneity. With the randomized field experiment setting in Section 2, we have three groups G_i based on two treatments (T_{1i} and T_{2i}) as follows:

$$G_i = \begin{cases} 1 & \text{if } T_{1i} = 0 \,\&\, T_{2i} = 0 \\ 2 & \text{if } T_{1i} = 1 \,\&\, T_{2i} = 0 \\ 3 & \text{if } T_{1i} = 1 \,\&\, T_{2i} = 1 \end{cases} . \tag{1}$$

where $T_{1i} = 1$ indicates that organization i receives treatment emails and $T_{2i} = 1$ indicates that organization i 's spam information and peer ranking is publicized in the treatment website. We run regressions of pre-experimental characteristics of organizations on the treatment assignments using

the following regression:

$$X_i = \theta_0 + \theta_1 T_{1i} + \theta_2 T_{2i} + \phi_i, \quad \phi_i \sim N(0, \sigma^2) \tag{2}$$

where X_i represents organization i's character before the experiment, T_{1i} is a dummy variable indicating whether organization i is privately treated or not, and T_{2i} is the public treatment dummy. We also apply Kolmogorov-Smirnov test and calculate the difference in the normalized standard deviation to check the balance based on the whole distribution. The results are shown in Table 2. We see that the differences of the average characteristics between the treatment and control groups are marginal and none of them is statistically significant. Therefore, our randomization satisfies the assumption of exogeneity.

5.3 Empirical Results

5.3.1 Basic analysis on spam volume

Since the distribution of the dependent variable spam volume is censored at 0. In fact, about 40% of the observations in our data set do not have any spam volume within at least one time period. As a result, normal distribution assumption in OLS regression could not be satisfied with our data set. As a result, we use Tobit model to estimate the coefficients in our model as follows:

$$Y_i = \begin{cases} Y_i^* & \text{if } Y_i > 0 \\ 0 & \text{if } Y_i \leq 0 \end{cases}$$

where $Y_i^*$is a latent variable:

$$Y_i^* = \alpha_0 + \alpha_1 T_{1i} + \alpha_2 T_{2i} + \alpha_3 * X_i + \epsilon_{1i}, \ \epsilon_{1i} \sim N(0, \sigma_1^2) \tag{3}$$

where Y_i is the spam volume for organization i at time t,X_i is the k-dimensional vector that represents organization i's characteristics such as pre-experimental spam volume, pre-experimental number of spamming IP addresses, number of IP addresses, number of IP addresses squared, whether the organization is publicly traded or not, number of observed botnets, and industry fixed effect. Also α_3 is the k-dimensional coefficient vector for the characteristics and ε_{1i} is the random error.

	No control		Industry fixed effects		K-S prob.		Ln(S_t/S_c)	
Dependent variables	Private	Public	Private	Public	Private	Public	Private	Public
Pre-experimental	-0.000164	-0.005447	-0.004760	-0.005676	1.000	0.998	0.008146	0.01713
Spam volume	(0.03833)	(0.03646)	(0.03542)	(0.03357)				
Pre-experimental number	-0.005479	0.0009089	-0.009958	-0.0006569	1.000	0.997	-0.01454	0.01798
of infesting IP addresses	(0.02933)	(0.01993)	(0.02791)	(0.01989)				
Number of IP addresses	-0.03488	0.02178	-0.04225	0.01687	0.891	0.997	-0.02775	-0.03337
	(0.04453)	(0.04150)	(0.04199)	(0.03893)				
Number of botnets	0.003922	-0.005299	0.001906	-0.003606	1.000	1.000	-0.001125	0.02757
	(0.04076)	(0.03692)	(0.03943)	(0.03397)				
Publicly trades or not	-0.001447	-0.006752	-0.002063	-0.007416	1.000	1.000	-0.01439	-0.06947
(=1 if yes)	(0.007068)	(0.007045)	(0.007019)	(0.007163)				

Table 2: Baseline comparison

a

[a]Note: This table presents comparisons of organizations' characteristics in the control and treatment groups. Columns 1 and 3 contain estimates of the average differences in characteristics between the control and private treatment organizations, without controls and with industry group fixed effects. Columns 2 and 4 contain estimates of the average differences in characteristics between the control and public treatment organizations, without controls and with industry group fixed effects. Columns 5 and 6 contain statistics from Kolmogorov-Smirnov test. Columns 7 and 8 contain the differences in normalized standard deviations between the treatment and control groups. Standard errors are clustered by industry group and shown in parentheses. * indicates statistical significance at the 10% level, ** at the 5% percent level, and *** at the 1% level.

Column 1-2 in Table 3 present the results from the regression model above. As expected, all treatment effects are negative, and the magnitudes of public treatment effects are larger than that of the private treatment group. However, the treatment effects lack statistical significance. The potential reason to explain the insignificance can be the heterogenous treatment effects among organizations. As we observed in Figure 4, only large spammers tend to decrease their spam volume after our intervention. Smaller spammers, especially for the initial "clean companies", their spam volume actually increased. To see how the treatment effects vary among different organizations, we further divide the organizations into four quantiles according to their initial spam volume and try to estimate the treatment effect for organizations in each quantile. For group 1, organizations' initial spam volume is 0; For group 2, their initial spam volume is positive, but less than 3 spams a month on average; For group 3, their initial spam volume is less than 48; And the rest organizations are in group 4. The results are presented in Column 3-6 in Table 3 and Figure 6.

With control variables, only public treatment effects for the top 25% spammers are significantly negative. On average, compared to the control group, organizations in the public group sent out only about 30% of spam volume. The result support Hypothesis 2 as well as Hypothesis 3. The coefficient of the private treatment effect is negative but not significant, indicating that treatment emails alone lacks effectiveness in spam reduction. The fact that only the public treatment group has a significant treatment effect shows that information sharing alone is not enough to change organizational behavior on security measures. The combination of information sharing and public announcement provides more economic motivation to the organizations. Most coefficients of the control variables are significant with expected signs. Organizations with more pre-experimental spam volume and botnets generally have more post-experimental spam volume, which can be an evidence that spam volume is a consistent indicator for organizational latent security level. In addition, we found that the relationship between spam volume and number of IP addresses is concave. As the number of IP addresses increase, spam volume first increases, then it decreases. The estimated largest spam volume is an organization with about 60,000 IP addresses. It can be explained by the fact that organizations with larger Internet space are facing more cybersecurity risks. However, largest organizations also have stronger security protection since many of them are companies in the high-tech industry and they have more resources to invest on security. As discussed before, institutions with large IP counts generally have more potential targets for bot herders and

it costs more to maintain and protect the system. The control variable "stock" represents whether the organization is publicly traded or not. Data shows that public companies tend to send out more spam volume though the results are not robust. We controlled industry variables for organizations with 3-digit NAICS and 2-digit SIC codes and there are no significant differences in the estimation results for either specification.

Our treatment effects can be further amplified with proposed nationwide independent institution due to the limitations in the present experiment. The first limitation is the visibility of our website. We had limited time to promote our website to attract more attention, which may have undermined our treatment effect given that one important component is reputation effect. Also some organizations may not pay enough attention to our emails. Fortunately, this limitation will be largely alleviated if the website is sponsored by the government. Secondly, our experiment stopped after two waves of treatment emails. As a result, organizations only got two treatment emails at the end of January and March 2014 respectively. With constant and long time notifications, the influence of our treatment may increase overtime. To testify the second potential reason, we used post-experimental data from the two months right after treatment emails were sent (February and April 2014). The results are listed in Table 3 column 7-10. Compared with the results with full post-experimental data, the magnitudes of both private and public treatments have increased. In addition, private treatment effect is statistically significant at 10% level with controls. Our results indicate evidence to support Hypothesis 1 to certain extend.

5.3.2 Treatment effects across industries

Organizations in different industry sectors may make different decisions. One of the most important industrial characteristics is the concentration ratio. To estimate how the treatment effects vary with competitiveness level, we got the percent of output accounted for by the top 50, 20, and 8 companies from the U.S. census data in 2007.[22] With this additional variable, the sample size decreases to 6,724. With a larger percentage of output, the industry has a higher level of concentration ratio, meaning a lower level of competition. We added the interaction terms of treatment dummies and industry level concentration ratio in the regression. The estimated results are listed in Table 4. It seems that the relationship between spam volume performance and industry competitiveness is convex that the organizations with best spam performance are in the industry with relatively less competition.

[22]The data is organized by the 2017 NAICS codes except for mining (NAICS 21), construction (NAICS 23), management of companies and enterprises (NAICS 55), and public administration (NAICS 92).

	Post-experimental spam volume									
	overall		full sample by quantile				2-months by quantile			
Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Private treatment	-0.0243	-0.0114	-0.0735	-0.0729	-0.0613	-0.0887	-0.162	-0.163	-0.144*	-0.177**
	(0.148)	(0.0655)	(0.185)	(0.119)	(0.0713)	(0.0756)	(0.196)	(0.129)	(0.0746)	(0.0714)
Public treatment	-0.0740	-0.0675	-0.291	-0.281**	-0.275***	-0.299***	-0.316	-0.311**	-0.306***	-0.329***
	(0.148)	(0.0706)	(0.188)	(0.122)	(0.0790)	(0.109)	(0.196)	(0.131)	(0.0834)	(0.126)
Private treatment*Q1			0.0499	0.0588	0.0719	0.0796	0.0806	0.105	0.122	0.137
			(0.261)	(0.195)	(0.232)	(0.164)	(0.310)	(0.238)	(0.223)	(0.209)
Private treatment*Q2			-0.207	-0.119	-0.165	-0.170	-0.229	-0.115	-0.184	-0.187
			(0.375)	(0.310)	(0.289)	(0.292)	(0.460)	(0.381)	(0.344)	(0.374)
Private treatment*Q3			0.154	0.150	0.139	0.206	0.350	0.345*	0.346**	0.412**
			(0.233)	(0.168)	(0.131)	(0.126)	(0.260)	(0.193)	(0.151)	(0.196)
Public treatment*Q1			0.310	0.284	0.276	0.300	0.174	0.183	0.178	0.194
			(0.261)	(0.195)	(0.175)	(0.207)	(0.310)	(0.239)	(0.234)	(0.270)
Public treatment*Q2			0.164	0.168	0.175	0.163	0.423	0.395	0.384	0.391
			(0.373)	(0.309)	(0.250)	(0.235)	(0.449)	(0.372)	(0.288)	(0.303)
Public treatment*Q3			0.450*	0.421**	0.418***	0.427**	0.492*	0.457**	0.456**	0.464*
			(0.235)	(0.171)	(0.158)	(0.206)	(0.261)	(0.195)	(0.183)	(0.245)
Pre-experimental spam volume		0.702***		0.413***	0.421***	0.428***		0.437***	0.446***	0.452***
		(0.0269)		(0.0345)	(0.0224)	(0.0289)		(0.0361)	(0.0229)	(0.0333)
Number of IP addresses		1.693***		1.480***	1.432***	1.406***		1.412***	1.362***	1.336***
		(0.161)		(0.103)	(0.127)	(0.138)		(0.114)	(0.159)	(0.174)
Number of IP addresses^2		-0.0800***		-0.0684***	-0.0668***	-0.0657***		-0.0631***	-0.0621***	-0.0609***
		(0.00755)		(0.00560)	(0.00610)	(0.00682)		(0.00609)	(0.00739)	(0.00870)
Number of botnets		0.280***		0.378***	0.375***	0.370***		0.366***	0.365***	0.359***
		(0.0254)		(0.0257)	(0.0328)	(0.0324)		(0.0272)	(0.0372)	(0.0373)
Stock		0.328***		0.135	0.187*	0.196**		-0.0154	0.0826	0.0698
		(0.106)		(0.107)	(0.101)	(0.0997)		(0.132)	(0.126)	(0.115)
Intercept	0.886***	-9.099***	6.391***	-5.726***	-6.334***	-6.107***	6.074***	-6.008***	-7.362***	-7.193***
	(0.108)	(0.759)	(0.130)	(0.495)	(0.531)	(0.538)	(0.137)	(0.560)	(0.721)	(0.723)
Industry	no	2-digit SIC	no	no	2-digit SIC	3-digit NAICS	no	no	2-digit SIC	3-digit NAICS
Observations	7,919	7,919	7,919	7,919	7,919	7,919	7,919	7,919	7,919	7,919

Table 3: Baseline treatment effects

a

[a]Note: This table displays the estimated private and public treatment effects with Tobit model. Column 1-2 report the estimates of the differences between the spam volume of treatment groups and control controlling for pre-experimental spam volume, number of pre-experimental IP addresses, number of pre-experimental IP addresses squared, number of pre-experimental infesting botnets, whether or not publicly traded and industry fixed effects overall. Column 3-6 reports the estimates of the differences between the spam volume of treatment groups for organizations in each quantile defined by pre-experimental spam volume. Column 7-10 report the estimates of the treatment effects in each quantile using the spam data in Feb and April 2014. Standard errors are clustered by industry codes and shown in parentheses. * indicates statistical significance at the 10% level, ** at the 5% percent level, and *** at the 1% level.

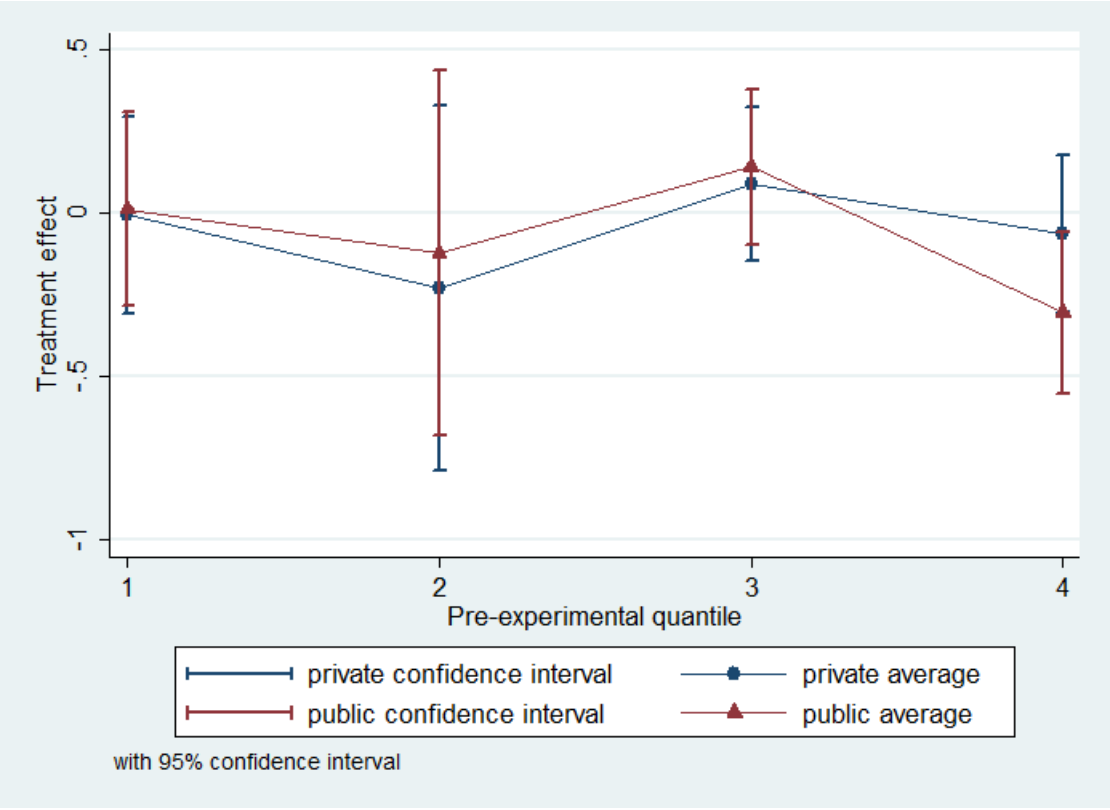


Figure 6: Treatment effects for organizations in each quantile

We observe that organizations in more concentrated industries tend to have more treatment effects. The results are not significant for the full sample, while they are significantly negative with the data from the months right after emails sending out. In addition, the magnitude of the private interaction treatment is larger than that for public one. We can explain the seemly counterintuitive results using Schumpeterian economic development theory (Schumpeter 1950). According to his theory, a more concentrated industry generally provides more profit and a more stable platform for organizations' innovations in that industry. When the general public does not pay enough attention to the security issues, the benefit from the investment on improving Internet security is uncertain. Companies, from highly competitive industries may take a risk to reduce their cost in order to get favorable positions in the competition. Organizations from more concentrated industries, however, have extra profit to improve the Internet security and reduce potential risk. This property is particularly significant for organizations in the private treatment group. Without the fear of being exposed to the public, the expected benefit of improving Internet security is limited, leading to a more evident difference between organizations from industries of different competition levels.

5.3.3 Peer effect analysis with excess-variance approach

From the previous results, we see that organizations will improve their security conditions by reducing outbound spam volume with security information publicity. However, more analysis should be done to recover the underlying mechanisms of organizations' security strategies. Organizations may improve their security protection due to the shame of being a "spammer". On the other hand, they may also change their strategies due to the "peer pressure" from their close competitors. If their customers and investors know that other similar organizations do better on security, they may shift to those companies.

Researchers have investigated peer effects in wide variety of individual and corporate outcomes, including academic achievement (Sacerdote 2001), product adoption (Aral and Walker 2012), stock market behavior (Brown et al. 2008), dividend payment (Popadak 2014), and managerial decision making (Shue 2013). With our "peer ranking" information available, we provide organizations a convenient way to compare their security levels with their peers, thus enhancing the peer influence in the security management. The existence of peer effect is important in understanding organizations' security strategies. If peer effect is important, then providing more comparisons between peers

	Full sample			Two months		
Variables	Top 50	Top 20	Top 8	Top 50	Top 20	Top 8
Private treatment	0.0888	0.0812	0.0888	0.183**	0.168**	0.159**
	(0.117)	(0.101)	(0.0882)	(0.0899)	(0.0762)	(0.0680)
Public treatment	0.0749	0.0431	0.0355	0.118	0.0840	0.0664
	(0.118)	(0.102)	(0.0889)	(0.0936)	(0.0813)	(0.0721)
Concentration ratio	-0.00772	-0.127***	-0.226***	-0.0160***	-0.127***	-0.213***
	(0.0193)	(0.0108)	(0.0149)	(0.00291)	(0.00352)	(0.00525)
Concentration ratio squared	7.54*e-5	0.000856***	0.00189***	0.000315***	0.000953***	0.00187***
	(0.000154)	(9.88e-05)	(0.000143)	(3.69*e-5)	(2.54e-05)	(4.33e-05)
Concentration ratio	-0.00197	-0.00222	-0.00313	-0.00355**	-0.00395***	-0.00496***
× Private treatment	(0.00206)	(0.00212)	(0.00237)	(0.00151)	(0.00138)	(0.00143)
Concentration ratio	-0.00227	-0.00204	-0.00244	-0.00301**	-0.00288*	-0.00327*
× Public treatment	(0.00208)	(0.00214)	(0.00239)	(0.00152)	(0.00151)	(0.00167)
Other characteristics	yes	yes	yes	yes	yes	yes
Industry	4-digit NAICS	4-digit NAICS	4-digit NAICS	4-digit NAICS	4-digit NAICS	4-digit NAICS
Observations	6,724	6,724	6,724	6,724	6,724	6,724
R-squared	0.757	0.757	0.757	0.754	0.754	0.754

Table 4: Treatment effects across industries

a

[a]Note: This table displays the estimated private and public treatment effects across industries with different levels of competition. Columns 1-3 report the estimates of the treatment effects with the cross products of treatments and industry's concentration ratio with the whole sample controlling for pre-experimental spam volume, number of pre-experimental IP addresses, number of pre-experimental IP addresses squared, number of pre-experimental infesting botnets, whether or not publicly traded, and 4-digit NAICS codes. Columns 4-6 report the estimates of the treatment effects with the cross products of treatments and industry's concentration ratio with the two months data right after treatment emails are sent. The differences among four columns are the measures of concentration ratio for each industry. For each column, we use the percent of output accounted for by the largest 50, 20, and 8 companies from the U.S. census data. Standard errors are clustered by industry codes and shown in parentheses. * indicates statistical significance at the 10% level, ** at the 5% percent level, and *** at the 1% level.

may be more effective to push organizations to invest resources on their security protection. At the same time, organizations with strong security protection may lack motivations to correct the existing problems due to the fact that they have already been in the lead. As found in Section 5.3.1, organizations with larger initial spam volume tend to be more responsive to our treatments.

Peer effect exists if organizations' behaviors are influenced by other peers' mean outcomes, which is, in our context, representing the industry sector's behavior. The identification of peer effects is difficult due to the reflection problem, unobservable variables, and selection problem (Manski 1993). To overcome the difficulties, the first identification strategy we used for the existence and magnitude of peer effects is the excess-variance approach (Graham 2008; Popadak 2014). The main idea of this method is to take advantage of various size for each industry group and the mathematical identity that the variance and size do not change in the same proportion. The intuition is as follows. The unconditional between-group variance is equal to the sum of the variance of group-level heterogeneity (different industrial characteristics), between-group variance of individual-level heterogeneity (average organizations' characteristics), and the strength of peer effect. With different sizes of industries, while the distribution of group-level heterogeneity is the same, we can use a method similar to "difference-in-differences" to compare the between- and within- group variance from different size's industries to estimate the peer effect. Due to the fact that organizations are not randomly assigned to different industry groups, the main issue for applying this identification method is that the results may be biased if self-selection also makes the variance to change inproportianal to group size. We believe that that it is not a main issue to be considered since Internet security is not a major concern for organizations' decision to enter the market. And it is difficult to imagine that organizations will sort them into peer groups differently based on the groups sizes. For example, financial services, retail organizations, and Internet service provider will face a high risk of potential security attack, but the sizes of the three industry groups vary a lot.

With the typical linear-in-means model (Manski 1993), organization i's spam behavior from industry j, D_{ij}, will be:

$$D_{ij} = \alpha_j + (\gamma - 1)\bar{\epsilon}_j + \epsilon_{ij} \tag{4}$$

where α_j represents industry-level heterogeneity, ϵ_{ij} represents organizational-level heterogeneity, and $\bar{\epsilon}_j$ represents the industry mean of the firm-level heterogeneity. So γ is the peer effect parameter

	Number of spam volume		Number of spamming hosts	
	SIC	NAICS	SIC	NAICS
γ^2	2.021	2.179	2.095	2.682
P-value $H_0: \gamma^2 = 1$	0.0002***	0.0084***	0.0000***	0.0004***
γ	1.422	1.476	1.447	1.638
Organization-specific covariates	Yes	Yes	Yes	Yes
Peer organization average covariates	Yes	Yes	Yes	Yes
Observations	7,919	7,919	7,919	7,919

Table 5: Peer effect analysis on spam volume

[a]

[a]This table displays the estimated peer effect using excess variance approach. Columns 1-2 represent the results using outbound spam volume. Columns 3-4 represent the results using number of spamming hosts. We use 2-digit SIC and NAICS codes to define peer groups. We use bootstrap to test the null hypothesis of no peer effects for 5000 samples. * indicates statistical significance at the 10% level, ** at the 5% percent level, and *** at the 1% level.

to be estimated. If $\gamma > 1$, then organizations' Internet security levels are influenced by their peers. As in Graham (2008) and Popadak (2014), the square of the peer influence, γ^2, can be identified as follows:

$$\frac{E[V_j^b|S_j = 1] - E[V_j^b|S_j = 0]}{E[V_j^w|S_j = 1] - E[V_j^w|S_j = 0]} = \gamma^2 \tag{5}$$

where S_j indicates whether industry j's type (large or small), and V_j^b and V_j^w represent the between-group variance and within-group variance for industry j. In the empirical analysis, we define $S_j = 1$ if the size of industry j is equal to or larger than the median size of all industries in our data set, and $S_j = 0$ otherwise. To exclude other characteristics, the variation attributed to other organizational and industry level average characteristics is removed first.

The results from the excess-variance approach for spam volume are listed in Table 5. Since we report the peer rankings in the treatments (emails and website) using the peer group defined by the 2-digit SIC and NAICS industry codes, we define organizations sharing the same 2-digit SIC and NAICS industry codes to be in the same peer group. The estimated γ^2 is about 2, which is statistically different from 1 using bootstrap, rejecting the null hypothesis that there is no peer effect. Our results support the Hypothesis 5 that there is peer effect among organizations within the same industry group.

5.3.4 Peer effect analysis with pairs distance metric

The second method we used to estimate peer effect is the pairs distance metric in Fracassi (2012) and Shue (2013). Since only the organizations in the private and public treatment groups received the treatment emails, we would expect that organizations in the two groups will present a larger peer effect. The two-stage procedure is as follows:

$$\text{1st Stage}: \ Y_{ij} = \alpha_0 + \alpha_1 X_{ij} + \tilde{Y_{ij}} \tag{6}$$

$$\text{2rd Stage}: \ |\tilde{Y_{ij}} - \tilde{Y_{kj}}| = \beta_0 + \beta_1 T_1 + \beta_2 T_2 + \epsilon_{ikj}. \tag{7}$$

For the first stage, we exclude the spam performance's variation from control variables, including all the control variables used above and the corresponding industry level characteristics. Y_{ij} measures the post-experimental spam volume, X_{ij} is organizations' characteristics, $\tilde{Y_{ij}}$ measures the unexplained component of variation. In the second stage, T_1 is a dummy variable whose value is 1 if only one of the organizations i and k in industry j is from the treatment group, and 0 otherwise. Similarly, T_2 is a dummy variable whose value is 1 if both of the organizations i and k in industry j are from the treatment group, and 0 otherwise. The intuition is that if organizations' spam performance is influenced by their peers in the industry, then the distances between organizations' unexplained part will be shorter. Taking advantage of the random assignment, if organizations from the treatment groups are more clustered compared to those in the control, then we can attribute the difference to our random treatment without selection bias.

In the analysis, we create all possible pairs of organizations within the same industry. And each observation in the second stage is one pair of organizations in the same industry. The informative statistic is the distance ratio as follows:

$$\begin{aligned} \text{Distance Ratio for control group} \quad \delta_1 &= 1 - \frac{E[|y_{ijc} - y_{ijc}|]}{E[|y_{ijt} - y_{ijc}|]} \\ \hat{\delta_1} &= -\frac{\beta_1}{\beta_0} \end{aligned} \tag{8}$$

$$\begin{aligned} \text{Distance Ratio for treatment group} \quad \delta_2 &= 1 - \frac{E[|y_{ijc} - y_{ijc}|]}{E[|y_{ijt} - y_{ijt}|]} \\ \hat{\delta_2} &= -\frac{\beta_2}{\beta_0} \end{aligned} \tag{9}$$

where y_{ijt} indicates the unexplained component of spam volume for the treated organization i in industry j and y_{ijc} indicates the unexplained component of spam volume for the controlled organization i in industry j. A significant positive $\hat{\delta_1}$ or $\hat{\delta_2}$ indicates the positive peer effect. The results of second stage are listed in Table 6. For the robustness, we estimated the distance ratio for both spam volume and number of spamming hosts. From the results, we find statistical significant positive peer effect in all specifications except for one estimate of $\hat{\delta_1}$. In addition, the absolute value of β_2 is larger than β_1 in all specifications, supporting Hypothesis 6 in Section 4.

6 Robustness Check

Our estimates are based on a large-scale randomized field experiment, which helps us to exclude the potential problems of omitted variables. But we conducted multiple robustness checks to provide more reliability of our estimates.

6.1 Placebo Test

Our experiment started at the end of January 2014. To testify the robustness of our estimated results, we assumed that our experiment started at the end of June, July, and August in 2013 and re-estimated our treatment effects. To be specific, we still use the six-month average spam volume before and after the assumed experimental start time. For the analysis started at the end of June and July, the post-experimental period will be from July 2013 to January 2014. As a result, we should not find any significant effect. For the analysis from August 2013 to Feb 2014, we may find some treatment effects but the magnitude should be smaller. The results are shown in Table 9 in Appendix 7. We can see that when the assumed start time is closer to our real time, the treatment effects get larger. More importantly, only the public treatment effects from column 6 is 10% level significant since our treatment started at Jan 2014. The results support that the spam reduction is actually from our intervention.

6.2 Subsample Analysis

An organization with zero pre-experimental spam volume could not decrease the spam volume any more and organizations with little spam have minor motivation to improve. Also tobit model has

	Spam volume				Number of spamming hosts			
	SIC		NAICS		SIC		NAICS	
β_0	1.786***	1.789***	1.744***	1.748***	-0.00838**	-0.00781**	-0.0109***	-0.0109***
	(0.00597)	(0.00488)	(0.00412)	(0.00413)	(0.00331)	(0.00331)	(0.00284)	(0.00284)
β_1	-0.0156***	-0.0272***	-0.00415	-0.00985*	-0.0103***	-0.00943***	-0.0213***	-0.0201***
	(0.00597)	(0.00597)	(0.00506)	(0.00506)	(0.00292)	(0.00292)	(0.00251)	(0.00251)
β_2	-0.0338***	-0.0339***	-0.0109***	-0.0163***	1.009***	1.009***	1.026***	1.025***
	(0.00526)	(0.00446)	(0.00445)	(0.00413)	(0.00270)	(0.00270)	(0.00233)	(0.00233)
F value $H_0: -\frac{\beta_1}{\beta_0} = 0$	6.88***	21.13***	0.68	3.82*	6.50**	5.64**	14.94***	14.83***
F value$H_0: -\frac{\beta_2}{\beta_0} = 0$	42.74***	42.56***	6.07**	13.59***	12.60***	10.62**	74.87***	66.25***
Organization-specific covariates	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Peer organization average covariates	No	Yes	No	Yes	No	Yes	No	Yes
Observations	1,033,676	1,403,432	1,033,676	1,403,432	1,033,676	1,403,432	1,033,676	1,403,432

Table 6: Pairs distance metric analysis

a

[a]This table displays the estimated peer effect using pairs distance metric approach. Columns 1-4 represent the results using spam volume data. Columns 5-8 represent the estimated results using number of spamming hosts. We use 2-digit SIC and NAICS codes to define peer groups. * indicates statistical significance at the 10% level, ** at the 5% percent level, and *** at the 1% level.

strong assumption on the distribution of the dependent variable. We re-estimated the regression using OLS model by only considering organizations that sent out positive pre-experimental spam volume or positive post-experimental spam volume. The results are presented in Table 10 in Appendix 7. The results confirm our main findings with whole sample.

6.3 Alternative Pre-experimental Spam Measure

In our experiment design and empirical analysis, we use the six-month average spam volume right before the start of the experiment as the control of the organization's original security condition. To test the robustness of our results, we re-ran the regression with two-month and four-month average spam volume. The results are presented in Table 11 in Appendix 7. We find similar treatment effects. The magnitudes of the public treatment effects are a little smaller. It may due to the fluctuation of spam volume over time.

6.4 Alternative Security Measure

We have multiple spam volume variables in our data set, we can do analysis using other spam volume measures to testify the robustness of our results. Despite the spam volume, number of infesting hosts is also important when we evaluate how bad one organization's security condition with regarding of outbound spam volume. In addition, we also have spam volume measure from another data source: Spamikaze's Passive Spam Block List (PSBL). The estimation results using number of infesting hosts from CBL and spam volume from PSBL are presented in Table 12 in Appendix 7. We can see with both dependent variables, large spammers in public treatment group tend to decrease their spam volume or spam hosts more compared to those in control group.

6.5 Data without ISPs

Since Internet service providers usually serve residential and business customers, they generally have different security policies and capabilities compared to other organizations in our data set. For example, they have less control over their customers' behavior on the Internet. Intuitively, we would expect them to be less responsive to our treatments. In our dataset, there are three industry groups that are related to Internet service providers: 6. telephone; 7. unclassified communication; 8. other communication. As a result, we reestimate the regressions using observations without those

three groups and the results are listed in Table 13 in Appendix 7. We can see, as we expect, the magnitudes of the public treatment effects are larger and more significant.

7 Concluding Remarks

Internet insecurity has been a serious problem, which calls for efforts from both researchers and governments. However, the current legal regime with passive and reactive security information disclosure is not sufficient to resolve the problem. In the present paper, we propose to set up a government sponsored third party institution to proactively monitor and publish organizations' security evaluation reports periodically to alleviate the threat. In order to evaluate the effectiveness of such an institution with corresponding security policy, we conducted a randomized field experiment with spam information disclosure on 7,919 U.S. organizations. The results show that the combination of information and publicity treatment significantly decrease large spammers' outbound spam volume, while information awareness treatment alone is not effective in decreasing spam volume. In addition, our experiment interference enhances the peer effects among organizations within the same industry, especially for those in the treatment groups. The significant existence of peer effect indicates that one of the spam reduction motivations is "peer pressure" from close competitors.

Our current experiment is just a starting point for the Internet security policy evaluation. It can be further extended to more experiments with other security information and in other economic environments. First, organizational security level is essentially a latent variable, which needs to be estimated by public data sources that can be measured even without the audit of target organizations. In addition to the outbound spam volume, phishing data and DDoS attacks can be other sources to estimate the latent variable. In our ongoing project, we are trying to construct other security evaluation metrics and empirically measure whether those also have consistent effects with that from spam information. Secondly, similar field experiments could be done in other countries with different political, social, and cultural backgrounds. Efficient designs or regulations in the U.S. may not work out in other countries as in Kugler (2014). Considering the fact that Internet security is an international issue and it has negative externality, it is necessary and beneficial for all countries to work on this problem together. Each country may conduct similar experiments and find effective ways to incentivize organizations to improve their security levels. Recently, we have started the

corresponding experiments in China and Korea with the cooperation with local researchers.

Regarding the treatment channel, social media can be used to deliver security reports to the treated organizations and the public. Social media, such as Facebook and Twitter, accounts for the top Internet activity according to Business Insider Intelligence.[23] Companies and organizations tend to open up social media accounts to publicize information and keep connected with their customers. For example, Facebook announced that it has 30 million business accounts as of June 2014. It will be helpful to set up a treatment homepage on popular social media and directly contact treated organizations via hashtags, posts, or direct messages. This approach may strengthen the economic motivation and treatment effects of the target security evaluation institute.

The proposed independent institution also provides a robust security metric with multiple aspects of security information including outbound spam, phishing, denial-of-service attack and so on. With the constructed security evaluation method, the government and independent institution can have a comprehensive understanding of the latent security condition for each organization, which is essential for cyber insurance. Without complete information, a competitive insurance market may not reach a steady state as in Rothschild and Stiglitz (1992). More importantly, the security evaluation information can attribute to set insurance premiums, just as automobile insurance companies have set up insurance premiums based on a driver's driving record.

Last but not least, we can incorporate the behaviors of bot herders, who are independent adverse strategic players, in the experiment. As noted by Anderson (2013), bot herders seek to maximize the profit on the black market and they would strategically choose victims according to the costs and benefits. One caveat of our paper is that publicized spam information may also change bot herder behaviors. For example, they may shift targets from treated organizations to untreated ones with the expectation that treated ones may pay more attentions to the security issues. If that is the case, the observed spam reduction for publicly treated organizations can not only be the result of security improvement but also of bot herders shifting targets. To detect this potential shifting, we keep track of every visitor's behavior flow on the website using Google Analytics. Also our current dataset contains botnet to ASN mappings, which allows us to do further analysis on bot herders' behavior.

[23] http://www.businessinsider.com/social-media-engagement-statistics-2013-12

References

[1] Adelsman, Rony M., and Andrew B. Whinston (1977). "Sophisticated voting with information for two voting functions." Journal of Economic Theory 15, no. 1: pp. 145-159.

[2] Anderson, Axel and Lones Smith. "Dynamic Deception." American Economic Review 103, no. 7 (2013): 2811-47.

[3] Anderson, Ross (2001). "Why information security is hard: An economic perspective." IEEE Computer Security Applications Conference, pp. 358-365.

[4] Aral, Sinan, and Dylan Walker. "Identifying influential and susceptible members of social networks." Science 337, no. 6092 (2012): pp. 337-341.

[5] Arora, Ashish, Ramayya Krishnan, Anand Nandkumar, Rahul Telang, and Yubao Yang (2004). "Impact of vulnerability disclosure and patch availability-an empirical analysis." Workshop on Economics of Information Security, vol. 24, pp. 1268-1287.

[6] Bauer, Johannes and Michael van Eeten (2009). "Cybersecurity: Stakeholder incentives, externalities, and policy options." Telecommunications Policy, Vol. 33, pp. 706-719.

[7] Blei, David M., Andrew Y. Ng, and Michael I. Jordan (2003). "Latent dirichlet allocation." Journal of Machine Learning Research 3: pp. 993-1022.

[8] Bratko, Andrej, Gordon V. Cormack, Bogdan Filipic, Thomas R. Lynam, and Blaz Zupan (2006). "Spam filtering using statistical data compression methods." Journal of Machine Learning Research 6: pp. 2673-2698.

[9] Bruhn, Miriam and David McKenzie (2008). "In pursuit of balance: Randomization in practice in development field experiments." World Bank Policy Research Working Paper Series.

[10] Casey, Eoghan (2011). Digital evidence and computer crime: Forensic science, computers and the Internet. Academic Press.

[11] Cormack, Gordon V., and Thomas R. Lynam (2007). "Online supervised spam filter evaluation." ACM Transaction on Information Systems, Vol. 25(3).

[12] D'Arcy, John, Anat Hovav, and Dennis Galletta (2009). "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach." Information Systems Research 20, no. 1: pp. 79-98.

[13] Denning, Dorothy E. (1987). "An intrusion-detection model." IEEE Transactions on Software Engineering, Vol. 13(2): pp. 222-232.

[14] Dharmapurikar, Sarang, Praveen Krishnamurthy, and David E. Taylor (2003). "Longest prefix matching using bloom filters." Proceedings of the ACM SIGCOMM Conference: pp. 201-212.

[15] Dice, Lee R. (1945). "Measures of the amount of ecologic association between species." Ecology 26(3): pp. 297-302.

[16] Duflo, Esther, Rachel Glennerster, and Michael Kremer (2007). "Using randomization in development economics research: A toolkit." Handbook of development economics 4 : 3895-3962.

[17] Fracassi, Cesare (2014). "Corporate finance policies and social networks." In AFA 2011 Denver Meetings Paper.

[18] Festinger, Leon (1954). "A theory of social comparison processes." Human relations 7, no. 2 : 117-140.

[19] Gal-Or, Esther, and Anindya Ghose (2005). "The economic incentives for sharing security information." Information Systems Research 16, no. 2: pp. 186-208.

[20] Graham, Bryan S. (2008). "Identifying social interactions through conditional variance restrictions." Econometrica 76, no. 3: pp. 643-660.

[21] Harper, Yan Chen, F. Maxwell, Joseph Konstan, and Sherry Xin Li (2010). "Social comparisons and contributions to online communities: A field experiment on movielens." The American economic review : 1358-1398.

[22] Harrison, Glenn W. and John A. List (2004). "Field experiments." Journal of Economic Literature: pp. 1009-1055.

[23] Kugler, Logan (2014). "Online Privacy: Regional Differences." Communications of the ACM, Vol. 58 No. 2, pp. 18-20.

[24] Krebs, Brian (2014). Spam Nation: The Inside Story of Organized Cybercrime - from Global Epidemic to Your Front Door. Sourcebooks, Inc.

[25] Lee, Wenke and Salvatore J. Stolfo (1998). "Data mining approaches for intrusion detection." Proceedings of 7th USENIX Security Symposium.

[26] Levchenko, Kirill, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Márk Félegyházi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage (2011). "Click Trajectories: End-to-End Analysis of the Spam Value Chain." IEEE Symposium on Security and Privacy.

[27] Moore, Tyler and Richard Clayton (2011). "The Impact of Public Information on Phishing Attack and Defense." Communications & Strategies 81.

[28] Morgan, Kari Lock, and Donald B. Rubin (2012). "Rerandomization to improve covariate balance in experiments." Annals of Statistics 40, no. 2: pp. 1263-1282.

[29] Popadak, Jillian A. (2012). "Dividend Payments as a Response to Peer Influence." Available at SSRN 2170561, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2170561.

[30] Pitsillidis, Andreas, Chris Kanich, Geoffrey M Voelker, Kirill Levchenko, Stefan Savage (2012). "Taster's choice: A comparative analysis of spam feeds." Proceedings of the 2012 ACM Internet Meassure Conference: pp. 427-440.

[31] Rao, Justin M. and David H. Reiley (2012). "The economics of spam." Journal of Economic Perspectives 26, no. 3: pp. 87-110.

[32] Roesch, Martin (1999). "SNORT: Lightweight intrusion detection for networks." Proceedings of 13th Large Installation System Administration Conference, pp. 229-238.

[33] Rossow, Christian (2014). "Amplification Hell: Revisiting Network Protocols for DDoS Abuse." Proceedings of Network and Distributed System Security Symposium.

[34] Rothschild, Michael and Joseph Stiglitz (1992). "Equilibrium in competitive insurance markets: An essay on the economics of imperfect information." Springer Netherlands.

[35] Sahami, Mehran, Susan Dumais, David Heckerman, and Eric Horvitz (1998). “A Bayesian approach to filtering junk e-mail.” Learning for Text Categorization 62: pp. 98-105.

[36] Shue, Kelly (2013). "Executive networks and firm policies: Evidence from the random assignment of MBA peers." Review of Financial Studies 26, no. 6: pp. 1401-1442.

[37] Stone-Gross, Brett, Christopher Kruegel, Kevin C. Almeroth, Andreas Moser, and Engin Kirda (2009). “FIRE: Finding rogue networks.” Proceedings of Annual Computer Security Applications Conference.

[38] Tang, Qian, John S. Quarterman, and Andrew B. Whinston (2013). “Improving Internet security through social information and social comparison: A field quasi-experiment.” In Workshop on the Economics of Information Security.

[39] Taylor, Robert W., Eric J. Fritsch, and John Liederbach (2014). Digital crime and digital terrorism. Prentice Hall Press.

[40] van Eeten, M., H. Asghari, J. M. Bauer, and S. Tabatabaie (2011). "Internet service providers and botnet mitigation: A fact-finding study on the Dutch market." Delft University of Technology.

[41] Vasek, Marie and Tyler Moore (2012). “Do malware reports expedite cleanup? An experimental study.” Workshop on Cyber Security Experimentation and Test.

[42] Wood, Dallas and Brent Rowe (2011). "Assessing home Internet users' demand for security: Will they pay ISPs?" Workshop of Economics of Information Security.

[43] Zakir, Durumeric, James Kasten, David Adrian, J. Alex Halderman, Michael Bailey, Frank Li, Nicolas Weaver, Johanna Amann, Jethro Beekman, Mathias Payer, and Vern Paxson (2014). “The Matter of Heartbleed.” Proceedings of Internet Measurement Conference, pp. 475-488.

Appendix A. Randomization Details

To get reliable treatment effect estimation from a randomized field experiment, we conducted a stratified, pair-wise matching randomization on about 8,000 organizations (Morgan and Rubin 2012). Due to heterogeneity of legal regimes and economic environment across countries, we only included U.S. organizations in the present experiment.

Stratification

One of the standard approaches to avoiding imbalance is stratification on a few key characteristics (R. A. Fisher, 1935). In stratification, organizations will be randomly assigned to different treatment groups within each subgroup, defined by key characteristics. In our experiment, we defined 195 subgroups by SIC codes (39 industry sectors) and number of IP addresses (5 segments). The detailed industry and number of IP addresses groups are listed in Table 7 and Table 8. Despite the correlation between industry activities, we managed to divide firms into mostly equal sized groups in order to get precise estimation.

The rationale of choosing the two characteristics is as follows. First, organizations in different industries have different priorities on security. For example, security should be particularly important for software companies. Spammers may also have different incentives based on the "value" of the data that different companies maintain. In that sense, financial and health sectors may have a higher risk. Second, organization size may affect the approaches on the system protection. Organizations with a larger number of IP addresses, generally with larger size, may face more risks and potential problems. On the other hand, large organizations usually have an independent IT department with security experts. With more resources, large organizations can afford better anti-virus software or firewalls to prevent potential security attacks. Therefore, we divided the whole sample into five groups according to their IP address counts.

Pair-wise matching

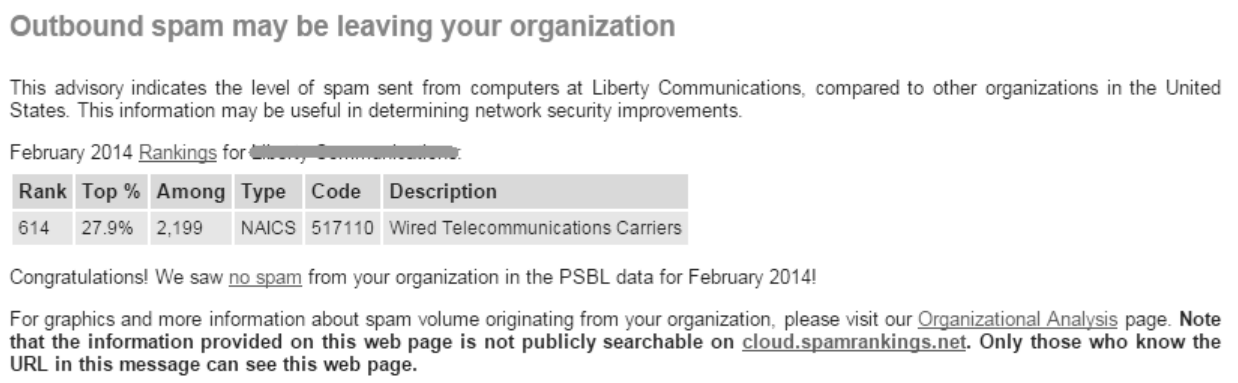
Stratification can only control for the balance of industry sectors and IP counts and the two variables cannot explain a large share of the spam volume's variance. Since the baseline spam volume can be the best proxy of the organizations' security condition, we did the pair-wise matching on

organizations' pre-experimental spam volume. In practice, we found three organizations that minimize the sum of three pairwise differences among them. One problem we faced during this process was the distribution of spam volume. We found that the distribution for a given organization varies greatly over time and both the distributions of spam volume and number of IP addresses for the whole sample were highly skewed. Thus, we used the natural logarithm transformed six month average spam volume as our pre-experimental spam volume to get higher probability of detecting the treatment effects.

Rerandomization

After the random assignment with stratification and pair-wise matching, we checked the distances between the control group and two treated groups with respect to companies' various characteristics. We followed the procedures in Morgan and Rubin (2012) to set the pre-specified criteria. With 10,000 simple random draws from our sample followed the previous two steps, we created a simulated distribution of distance between any two groups and set the 5% quantile as the criteria for randomization. Finally, with the 10,000 randomization assignments satisfying the rerandomization criteria for power calculation, we randomly chose one of them as our executed one.

Appendix B. Additional Figures and Tables



Outbound spam may be leaving your organization

This advisory indicates the level of spam sent from computers at Liberty Communications, compared to other organizations in the United States. This information may be useful in determining network security improvements.

February 2014 Rankings for [redacted]:

Rank	Top %	Among	Type	Code	Description
614	27.9%	2,199	NAICS	517110	Wired Telecommunications Carriers

Congratulations! We saw no spam from your organization in the PSBL data for February 2014!

For graphics and more information about spam volume originating from your organization, please visit our Organizational Analysis page. **Note that the information provided on this web page is not publicly searchable on cloud.spamrankings.net. Only those who know the URL in this message can see this web page.**

(a) Treatment email for a privately treated organization

Outbound spam may be leaving your organization

This advisory indicates the level of spam sent from computers at Hurricane Electric Inc., compared to other organizations in the United States. This information may be useful in determining network security improvements.

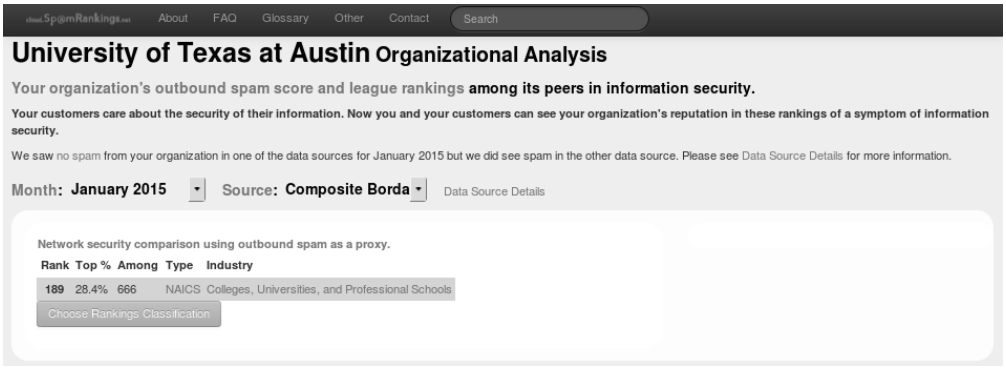
February 2014 Rankings for [redacted]:

Rank	Top %	Among	Type	Code	Description
61	2.8%	2,199	NAICS	517110	Wired Telecommunications Carriers

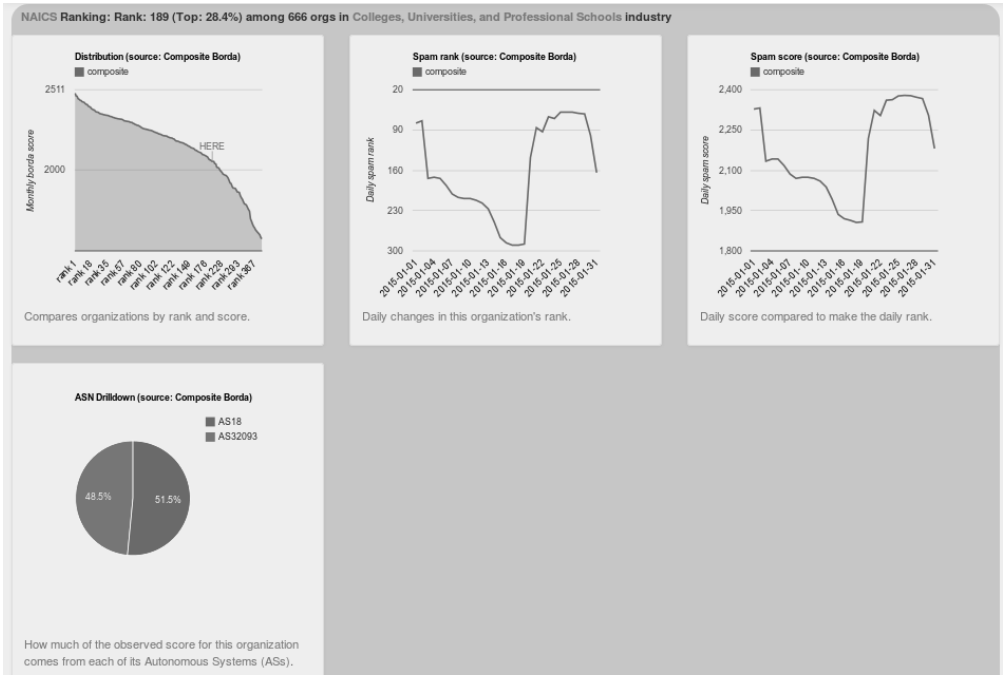
For graphics and more information about spam volume originating from your organization, please visit our Organizational Analysis page. **Note that the information provided on this web page is publicly searchable on cloud.spamrankings.net.**

(b) Treatment email for a publicly treated organization

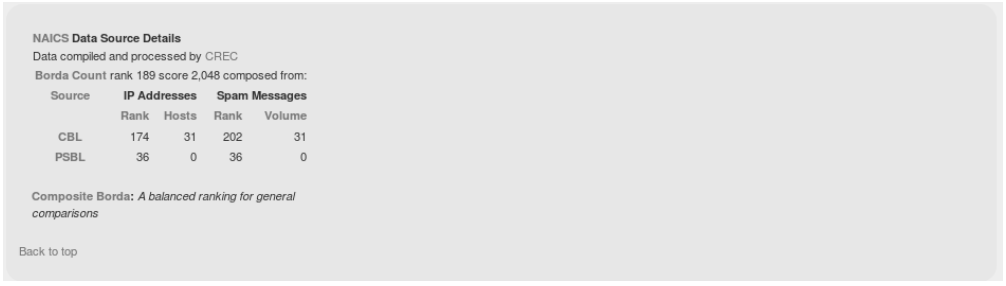
Figure 7: Examples of treatment emails



(a) Overview



(b) Distribution chart, time series, drilldowns



(c) Detailed source information

Figure 8: Details on the treatment website cloud.spamrankings.net

Group	Industry	Number of organizations
1	agriculture, mining and construction	123
2	electronic devices	103
3	publishing	133
4	chemical and measuring manufacturing	156
5	other manufacturing	245
6	telephone	836
7	unclassified communication	164
8	other communication	163
9	transportation	253
10	durable wholesale	215
11	non-durable wholesale	126
12	furniture retail	111
13	non-classified retail	145
14	other retail	158
15	depository institutions	186
16	credit and real estate	133
17	security	255
18	insurance	199
19	holdings and other financial companies	179
20	health service	337
21	colleges	423
22	education service other than colleges	214
23	management consulting	181
24	business consulting	150
25	other management service	116
26	engineer, accounting and research	194
27	non-classified business service	484
28	computer programming	249
29	prepackaged software	140
30	computer integrated systems	157
31	computer processing	162
32	information retrieval	102
33	non-classified computer service	167
34	other business service	222
35	legal service	108
36	membership organization	93
37	miscellaneous service	115
38	other service	223
39	public administration	199

Table 7: Industrial groups' description

number of IP addresses	0-427	427-1024	1024-10^4	10^4-10^5	>10^5
Group	1	2	3	4	5

Table 8: Groups based on number of IP addresses

	Post-experimental spam volume					
	June 2013		July 2013		August 2013	
Variables	(1)	(2)	(3)	(4)	(5)	(6)
Private treatment	0.0386	0.0561	-0.0116	0.0284	0.00112	0.000767
	(0.0491)	(0.119)	(0.0562)	(0.116)	(0.0522)	(0.0961)
Public treatment	-0.0101	-0.0833	-0.0645	-0.109	-0.0691	-0.184*
	(0.0539)	(0.146)	(0.0529)	(0.119)	(0.0576)	(0.111)
Private treatment*Q1		-0.148		0.120		0.0629
		(0.219)		(0.163)		(0.155)
Private treatment*Q2		0.0791		-0.210		-0.147
		(0.126)		(0.259)		(0.211)
Private treatment*Q3		-0.0595		-0.114		-0.0512
		(0.137)		(0.138)		(0.125)
Public treatment*Q1		0.102		0.230		0.152
		(0.231)		(0.174)		(0.167)
Public treatment*Q2		0.181		0.0539		0.0243
		(0.195)		(0.205)		(0.183)
Public treatment*Q3		0.0312		-0.0412		0.234*
		(0.168)		(0.132)		(0.133)
Pre-experimental spam volume	0.618***	0.432***	0.650***	0.470***	0.661***	0.409***
	(0.0384)	(0.0475)	(0.0400)	(0.0349)	(0.0348)	(0.0231)
Number of IP addresses	1.855***	1.684***	1.669***	1.460***	1.622***	1.370***
	(0.168)	(0.143)	(0.157)	(0.129)	(0.161)	(0.123)
Number of IP addresses^2	-0.0915***	-0.0836***	-0.0813***	-0.0714***	-0.0779***	-0.0662***
	(0.00858)	(0.00730)	(0.00825)	(0.00701)	(0.00839)	(0.00670)
Number of botnets	0.0412	-0.0180	0.149	0.0723	0.213**	0.130
	(0.111)	(0.0968)	(0.0946)	(0.0804)	(0.107)	(0.0882)
Stock	0.378***	0.445***	0.314***	0.377***	0.283***	0.368***
	(0.0645)	(0.0725)	(0.0519)	(0.0573)	(0.0372)	(0.0418)
Intercept	-9.311***	-6.932***	-8.679***	-6.538***	-8.557***	-5.568***
	(0.711)	(0.609)	(0.631)	(0.478)	(0.651)	(0.483)
Industry	2-digit SIC	2-digit SIC	2-digit SIC	2-digit SIC	2-digit SIC	2-digit SIC
Observations	7,919	7,919	7,919	7,919	7,919	7,919

Table 9: Placebo test

[a]

[a]Note: This table displays the robustness check with placebo test. Columns 1-2, 3-4, and 5-6 use October, November, and December as our experiment start time, respectively. All regressions are controlled for pre-experimental spam volume, number of pre-experimental IP addresses, number of pre-experimental IP addresses squared, number of pre-experimental infesting botnets, whether or not publicly traded and industry codes. Standard errors are clustered by industry codes and shown in parentheses. * indicates statistical significance at the 10% level, ** at the 5% percent level, and *** at the 1% level.

	Post-experimental spam volume					
	overall		full sample by quantile			
Variables	(1)	(2)	(3)	(4)	(5)	(6)
Private treatment	-0.0153	0.00122	-0.0630	-0.0705	-0.0683	-0.0939
	(0.108)	(0.0429)	(0.179)	(0.114)	(0.0689)	(0.0725)
Public treatment	-0.0561	-0.0601	-0.274	-0.271**	-0.273***	-0.292***
	(0.108)	(0.0528)	(0.181)	(0.117)	(0.0755)	(0.103)
Private treatment*Q1			0.118	0.133	0.229	0.240
			(0.223)	(0.180)	(0.169)	(0.169)
Private treatment*Q2			-0.0903	-0.0268	-0.0368	-0.0478
			(0.239)	(0.198)	(0.183)	(0.189)
Private treatment*Q3			0.108	0.121	0.120	0.166
			(0.206)	(0.146)	(0.112)	(0.102)
Public treatment*Q1			0.308	0.295*	0.329***	0.338**
			(0.218)	(0.174)	(0.119)	(0.152)
Public treatment*Q2			0.174	0.189	0.207	0.217
			(0.241)	(0.199)	(0.147)	(0.148)
Public treatment*Q3			0.380*	0.365**	0.366***	0.379**
			(0.209)	(0.149)	(0.129)	(0.175)
Pre-experimental spam volume		0.391***		0.399***	0.399***	0.405***
		(0.0256)		(0.0333)	(0.0211)	(0.0266)
Number of IP addresses		1.092***		1.146***	1.079***	1.081***
		(0.139)		(0.0901)	(0.125)	(0.124)
Number of IP addresses^2		-0.0511***		-0.0540***	-0.0507***	-0.0509***
		(0.00702)		(0.00498)	(0.00626)	(0.00625)
Number of botnets		0.383***		0.378***	0.370***	0.368***
		(0.0351)		(0.0249)	(0.0302)	(0.0291)
Stock		-0.0891		-0.0507	-0.0301	-0.00411
		(0.0808)		(0.0873)	(0.0835)	(0.0643)
Intercept	3.724***	-4.038***	6.433***	-3.745***	-3.493***	-3.515***
	(0.0763)	(0.608)	(0.126)	(0.431)	(0.499)	(0.507)
Industry	no	2-digit SIC	no	no	2-digit SIC	3-digit NAICS
Observations	5,284	5,284	5,284	5,284	5,284	5,284

Table 10: Treatment effects with subsample data

a

[a]Note: This table displays the robustness check with only organizations that sending out positive pre-experimental spam volume or positive post-experimental spam volume using OLS regression. Column 1-2 report the estimates of the differences between the spam volume of treatment groups and control controlling for pre-experimental spam volume, number of pre-experimental IP addresses, number of pre-experimental IP addresses squared, number of pre-experimental infesting botnets, whether or not publicly traded and industry fixed effects overall. Column 3-6 reports the estimates of the differences between the spam volume of treatment groups for organizations in each quantile defined by pre-experimental spam volume. Standard errors are clustered by industry codes and shown in parentheses. * indicates statistical significance at the 10% level, ** at the 5% percent level, and *** at the 1% level.

	Post-experimental spam volume							
	2-month average pre				4-month average pre			
Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Private treatment	-0.0303	-0.0625	-0.0506	-0.0776	-0.0228	-0.0614	-0.0492	-0.0741
	(0.0684)	(0.117)	(0.0721)	(0.0764)	(0.0641)	(0.117)	(0.0674)	(0.0679)
Public treatment	-0.0849	-0.249**	-0.246**	-0.264**	-0.0676	-0.224*	-0.220**	-0.239**
	(0.0737)	(0.119)	(0.107)	(0.114)	(0.0704)	(0.120)	(0.0926)	(0.105)
Private treatment*Q1		0.0485	0.0568	0.0657		0.0477	0.0571	0.0627
		(0.193)	(0.234)	(0.159)		(0.193)	(0.236)	(0.159)
Private treatment*Q2		-0.198	-0.232	-0.236		-0.199	-0.237	-0.244
		(0.309)	(0.266)	(0.285)		(0.308)	(0.264)	(0.270)
Private treatment*Q3		0.115	0.101	0.167		0.122	0.109	0.173
		(0.166)	(0.138)	(0.117)		(0.166)	(0.134)	(0.116)
Public treatment*Q1		0.252	0.246	0.266		0.228	0.221	0.241
		(0.192)	(0.199)	(0.214)		(0.192)	(0.191)	(0.211)
Public treatment*Q2		0.0968	0.112	0.0954		0.0722	0.0861	0.0686
		(0.306)	(0.252)	(0.238)		(0.306)	(0.246)	(0.233)
Public treatment*Q3		0.333**	0.334*	0.342*		0.312*	0.310*	0.318
		(0.169)	(0.189)	(0.206)		(0.169)	(0.183)	(0.208)
Pre-experimental spam volume	0.740***	0.435***	0.428***	0.427***	0.776***	0.483***	0.475***	0.475***
	(0.0437)	(0.0241)	(0.0409)	(0.0364)	(0.0431)	(0.0275)	(0.0416)	(0.0371)
Number of IP addresses	1.815***	1.404***	1.372***	1.353***	1.659***	1.424***	1.389***	1.371***
	(0.139)	(0.100)	(0.112)	(0.127)	(0.129)	(0.101)	(0.113)	(0.131)
Number of IP addresses^2	-0.0865***	-0.0649***	-0.0640***	-0.0631***	-0.0785***	-0.0660***	-0.0648***	-0.0640***
	(0.00644)	(0.00544)	(0.00539)	(0.00624)	(0.00594)	(0.00548)	(0.00537)	(0.00645)
Number of botnets	0.319***	0.372***	0.378***	0.377***	0.278***	0.358***	0.363***	0.362***
	(0.0520)	(0.0210)	(0.0473)	(0.0355)	(0.0452)	(0.0216)	(0.0483)	(0.0365)
Stock	0.255**	0.134	0.162	0.171	0.274***	0.152	0.174*	0.183*
	(0.114)	(0.108)	(0.107)	(0.111)	(0.104)	(0.107)	(0.103)	(0.105)
Intercept	-9.489***	-5.028***	-5.623***	-5.394***	-9.070***	-5.542***	-6.174***	-5.959***
	(0.676)	(0.476)	(0.526)	(0.546)	(0.649)	(0.483)	(0.554)	(0.580)
Observations	7,919	7,919	7,919	7,919	7,919	7,919	7,919	7,919

Table 11: Treatment effects with alternative measures of pre-experimental spam volume

a

[a]Note: This table displays the robustness check with alternative measures of pre-experimental spam volume. Columns 1-4 use monthly average spam volume from November 2013 to December 2013 while Columns 5-8 use monthly average spam volumn from September 2013 to December 2013. All columns are controlled for pre-experimental spam volume, number of pre-experimental IP addresses, number of pre-experimental IP addresses squared, number of pre-experimental infesting botnets, whether or not publicly traded, and industry codes. Standard errors are clustered by industry codes and shown in parentheses. * indicates statistical significance at the 10% level, ** at the 5% percent level, and *** at the 1% level.

	Post-experimental spam volume							
	number of infesting hosts by CBL				number of spam volume by PSBL			
Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Private treatment	-0.0271	-0.0179	-0.0557	-0.0366	-0.0321	-0.0206	-0.0663	-0.0777
	(0.0990)	(0.0447)	(0.107)	(0.0571)	(0.175)	(0.0923)	(0.195)	(0.124)
Public treatment	-0.0328	-0.0369	-0.101	-0.0983*	-0.132	-0.105	-0.315	-0.272**
	(0.0988)	(0.0451)	(0.107)	(0.0585)	(0.175)	(0.0915)	(0.195)	(0.122)
Private treatment*Q1			0.0262	0.0160			0.153	0.156
			(0.164)	(0.115)			(0.400)	(0.279)
Private treatment*Q2			-0.143	-0.105			0.217	0.164
			(0.243)	(0.194)			(0.598)	(0.430)
Private treatment*Q3			0.0906	0.0666			0.0647	0.0932
			(0.146)	(0.0980)			(0.331)	(0.229)
Public treatment*Q1			0.126	0.113			0.206	0.175
			(0.163)	(0.116)			(0.403)	(0.278)
Public treatment*Q2			0.0197	0.0183			0.672	0.484
			(0.243)	(0.194)			(0.610)	(0.442)
Public treatment*Q3			0.160	0.108			0.554*	0.425*
			(0.147)	(0.0987)			(0.328)	(0.225)
Pre-experimental spam volume		0.970***		0.736***		0.658***		0.602***
		(0.0202)		(0.0395)		(0.0421)		(0.0366)
Number of IP addresses		0.698***		0.663***		2.633***		1.514***
		(0.0579)		(0.0571)		(0.144)		(0.122)
Number of IP addresses^2		-0.0308***		-0.0286***		-0.128***		-0.0740***
		(0.00309)		(0.00303)		(0.00795)		(0.00642)
Number of botnets		0.0254**		0.0891***		0.455***		0.318***
		(0.0123)		(0.0155)		(0.0294)		(0.0229)
Stock		0.213***		0.148**		-0.510***		-0.323**
		(0.0635)		(0.0657)		(0.164)		(0.160)
Intercept	0.795***	-3.904***	4.366***	-2.942***	-3.683***	-14.99***	1.410***	-8.094***
	(0.0738)	(0.253)	(0.0739)	(0.271)	(0.153)	(0.665)	(0.137)	(0.610)
Observations	7,919	7,919	7,919	7,919	7,919	7,919	7,919	7,919

Table 12: Treatment effects with different security measures

a

[a]Note: This table displays the robustness check with different security measures. Column 1-4 report the treatment effects for number of infesting hosts by CBL in each quantile. Column 5-8 report the treatment effects for spam volume by PSBL in each quantile. The control variables include pre-experimental spam volume measures, number of pre-experimental IP addresses, number of pre-experimental IP addresses squared, number of pre-experimental infesting botnets, whether or not publicly traded.Standard errors are clustered by industry codes and shown in parentheses. * indicates statistical significance at the 10% level, ** at the 5% percent level, and *** at the 1% level.

	Post-experimental spam volume					
	overall		full sample by quantile			
Variables	(1)	(2)	(3)	(4)	(5)	(6)
Private treatment	0.0365	0.00153	0.0220	-0.0431	-0.0279	-0.0738
	(0.147)	(0.0785)	(0.221)	(0.156)	(0.111)	(0.106)
Public treatment	-0.0265	-0.0567	-0.304	-0.361**	-0.355***	-0.390***
	(0.147)	(0.0846)	(0.226)	(0.158)	(0.103)	(0.127)
Private treatment*Q1			-0.0185	0.0447	0.0568	0.0796
			(0.288)	(0.225)	(0.267)	(0.174)
Private treatment*Q2			-0.377	-0.241	-0.293	-0.279
			(0.395)	(0.337)	(0.280)	(0.312)
Private treatment*Q3			0.0806	0.126	0.110	0.197
			(0.264)	(0.200)	(0.173)	(0.153)
Public treatment*Q1			0.382	0.411*	0.401**	0.435**
			(0.291)	(0.225)	(0.181)	(0.198)
Public treatment*Q2			0.0164	0.108	0.120	0.121
			(0.398)	(0.338)	(0.274)	(0.269)
Public treatment*Q3			0.495*	0.518**	0.513***	0.528**
			(0.270)	(0.203)	(0.177)	(0.227)
Pre-experimental spam volume		0.708***		0.401***	0.416***	0.425***
		(0.0363)		(0.0467)	(0.0342)	(0.0421)
Number of IP addresses		1.555***		1.305***	1.305***	1.276***
		(0.189)		(0.120)	(0.151)	(0.174)
Number of IP addresses^2		-0.0731***		-0.0588***	-0.0601***	-0.0589***
		(0.00898)		(0.00663)	(0.00724)	(0.00881)
Number of botnets		0.339***		0.438***	0.449***	0.444***
		(0.0494)		(0.0453)	(0.0468)	(0.0321)
Stock		0.401***		0.200*	0.252***	0.268**
		(0.0904)		(0.111)	(0.0947)	(0.107)
Intercept	0.325***	-8.579***	5.625***	-5.167***	-6.012***	-5.770***
	(0.109)	(0.919)	(0.156)	(0.580)	(0.662)	(0.666)
Industry	no	2-digit SIC	no	no	2-digit SIC	3-digit NAICS
Observations	6,755	6,755	6,755	6,755	6,755	6,755

Table 13: Treatment effects without ISPs

a

[a]Note: This table displays the robustness check without ISPs' observations. Column 1-2 report the estimates of the differences between the spam volume of treatment groups and control controlling for pre-experimental spam volume, number of pre-experimental IP addresses, number of pre-experimental IP addresses squared, number of pre-experimental infesting botnets, whether or not publicly traded and industry fixed effects overall. Column 3-6 reports the estimates of the differences between the spam volume of treatment groups for organizations in each quantile defined by pre-experimental spam volume. Standard errors are clustered by industry codes and shown in parentheses. * indicates statistical significance at the 10% level, ** at the 5% percent level, and *** at the 1% level.