Information Disclosure and Security Policy Design: A Large-Scale Randomization Experiment in Pan-Asia

Yun-Sik Choi,[1] Shu He,[2] Yunhui Zhuang,[3]
Gene Moo Lee,[4] Chung Man Alvin Leung,[3] and Andrew B. Whinston[5]

Abstract

The ever increasing number of cyberattacks motivates us to explore a more effective way to enhance the security awareness of the organizations and the general public. Establishing a ranking scheme of firms against online scams may heighten such awareness to address suboptimal security issues. Recognizing the limited research in Pan-Asia, we are motivated to conduct an exploratory study to understand the cyber security issues in the region. The main objective of this study is to find how organizations react in managing two distinct security issues, spam emission and phishing website hosting, when (1) they become aware of such problems and (2) the information is publicized. We argue that spam emission can be considered as an indicator of improper internal control on botnet and malware infections as well as distorted incentives causing negative externality issues, while phishing website hosting behavior can be attributed as a pure negative externality issues caused by lack of deterrence policy and responsibility. To achieve the research goal, we conducted a randomized field experiment on a total population of 1,262 organizations in six Pan-Asian countries. To construct the organizational security evaluation reports, we collected data from four reputable sources and developed a public security advisory website and an email treatment system. With rigorous econometric analysis, we find heterogeneous treatment effects depending on the characteristics of security incidents. Based on the results, we propose cybersecurity policy directions to address the externality issue.

Keywords: cybersecurity; externality; policy design; spam; phishing; botnet; information security index; organizational security; randomized field experiment

[1] Computer Science Department, The University of Texas at Austin
[2] School of Business, University of Connecticut
[3] College of Business, City University of Hong Kong
[4] Sauder School of Business, University of British Columbia
[5] McCombs School of Business, The University of Texas at Austin

1. Introduction

Cyberattacks are imposing serious threats to individuals, organizations, and our society at large. Even with the technological advances in secure software and hardware, we are still experiencing an ever-increasing number of cyberattacks.[6] Anderson and Moore (2006) argued that this suboptimal situation in cyberspace is partly due to negative externalities, information asymmetry, and misaligned incentives. This motivates us to explore more effective measures to enhance the security awareness in both organizational and societal levels and to create proper incentives to achieve secure cyber environments. In a recent U.S.-based field experiment, He et al. (2016) showed that publicizing security ranking of organizations against email spam emission may heighten such organizational awareness towards security issues. Provided that cybersecurity is a global issue and each geographical region has its distinct economic and societal environments, there is a need to extend the economics of cybersecurity literature by incorporating international environments. Specifically, in this paper, we focus on Pan-Asia countries which show significant economic development as well as rapid adoption of technologies.

1.1 Cybercrime and Related Ordinances in Pan-Asian Countries

According to AIA's Landmark Healthy Living Survey, adults in Hong Kong spend an average of 3.7 hours per day on the Internet.[7] With increasing Internet users, cybercrime is becoming a growing concern. Several pieces of legislation introduced in Hong Kong are the Computer Crimes Ordinance enacted in 1993, the Telecommunications Ordinance (Cap. 106), Crimes Ordinance (Cap. 200) and Theft Ordinance (Cap. 210) which has been extended to cover computer crimes. However, these legislations have not been amended or updated for quite some time and are not particularly applicable against the modern and even complex cybercrime landscape. Another piece of legislation of relevance is the Unsolicited Electronic Message Ordinance (UEMO) enacted in 2007 to control for spam. However, there is no legislation that deals with other cybercrimes such as phishing. The Hong Kong Monetary Authority regularly issues statements warning against fraud and phishing cases. In 2015, the Legislative Council also cited phishing and botnets as the main causes for a 405% increase in IT security incidents over four years.[8] Considering that phishing has been recognized as a serious threat to businesses and households, it is rather surprising that there is still no direct legislation to deal with this kind of crime.

Japan has thorough anti-spam legislation in the Act on Regulation of Transmission of Specified Electronic Mail (2009) and has legislation applicable to phishing.[9] While the degree of legislation on cybercrime varies across Pan-Asia (see Appendix 1 for more information), countries such as South Korea, Singapore, and Malaysia have effective cybercrime legislation in place. They provide legislation covering an umbrella of generic cybercrime whilst also being applicable to more complex crimes such as fraud, spam and phishing. This balance between breadth and depth in legislation is something that Hong Kong

[6]Internet Security Threat Report 2017 ISTR:Vol.22, Symantec
https://www.symantec.com/security-center/threat-report
[7]http://www.aia.com.hk/en/about-aia/media-centre/press-releases/2016/hong-kongs-aia-healthy-living-index-ranking-drops-to-last-place-in-asia-pacific.html
[8]http://www.legco.gov.hk/research-publications/english/1617issh07-cyber-security-in-hong-kong-20161122-e.pdf
[9]http://measures.antispam.soumu.go.jp/pdf/Japanese%20anti-spam%20law.pdf

and countries in the region can learn from and adapt to its own legislation in the future to keep up with the complex and evolving nature of cybercrime.

1.2 Motivation and Contribution

Motivated by the unique nature and the increasing importance of Pan-Asian countries, we extend the work from He et al. (2016) by conducting a randomized experiment in this region to test the impact of security information publication on the security improvement. Specifically, we developed an information security score that reflects an organization's preparedness against cybercrimes. Similar to the idea of Moody's and Standard and Poor's credit ratings, we build a security evaluation system that can be used as an indicator of the security vulnerabilities of the organizations. The score is constructed from processing large-scale, real-time cyber incident data points from spam emission[10] (CBL[11], PSBL[12]) and phishing website hosting (APWG[13], OpenPhish[14]) activities.

We argue that organizations would tend to deprioritize security issues when the problems are less likely to directly harm themselves, even though they create negative externalities to the outside of the companies (Anderson and Moore 2006, van Eeten et al. 2007, Shetty et al. 2010). Spam and phishing cause significant cost to the email recipients and phishing website visitors, where a significant portion of them are re from the outside the organizations. However, there is a notable difference between sending out spam mails and hosting a phishing website. Most spam emails are being sent from Internet connected devices which are compromised by bots (Moore et al. 2009). Having bots installed on a company-owned machine may indicate that the organization is lack of proper security protection mechanisms . It also means that there is a high possibility of other malware[15] which can be used to harm internal system or steal sensitive data. Thus organizations generating large outbound spam volume can be regarded as ones with insecure information systems. According to our 2017 CBL spam feed,[16] we found that about 55.8% (585,808) among the spam emitting IP addresses (1,048,575) are infected by bots. Depending on the type of bots, the compromised machines can access and steal sensitive internal data and/or participate in DDoS attacks.

Comparing to spam, phishing websites[17] have different underlying mechanisms. While spam can be intermittently emitted by infected computers, phishing websites can only be hosted on dedicated web servers that are operated by the web hosting services. In other words, these phishing websites can be hosted on *legitimate* hosting services or hijacked websites, depending on the type of attackers. We argue that the organizations hosting phishing websites are more likely to have insufficient security policies and

---

[10] Note that the term 'spam mail' in this paper includes advertisement, phishing mail, and malware attached email.
[11] https://www.abuseat.org/
[12] https://psbl.org/about/
[13] https://www.antiphishing.org/
[14] https://openphish.com/
[15] https://ics-cert.us-cert.gov/sites/default/files/documents/NCCIC_ICS-CERT_AAL_Malware_Trends_Paper_S508C.pdf
[16] CBL provides source botnet information for each spam mail whenever it is available.
[17] In this paper, phishing exclusively refers website related incidents, and we only focus on the organizations who are actually hosting the phishing websites on their own server. All email related attack including phishing emails are included in our spam data.

moral hazard against externality (Anderson and Moore 2006; van Eeten and Bauer 2007).[18] According to our collected data in the focal Pan-Asian countries, we observe that, among 319 phishing URLs appearing more than three times during 2017, 41.8% of URLs were from legitimate domain (hijacked),[19] and 58.2% was self-registered,[20] or using free hosting companies' domains.[21] As phishing attacks involved with the use of legitimate web servers, we expect to observe a different treatment effect on the phishing website hosting, comparing to that of spam emission.

Based on collected spam and phishing data and the associated ranking, we conducted a large-scale randomized field experiment (RFE) to investigate whether informing and publicizing the proposed security score induces an improvement of the organizational security level, which can be measured by the number of reported cybercrime records originated from their networks after the interventions. To conduct a large-scale experiment, we developed a public treatment website, cybeRatings (https://cyberatings.is.cityu.edu.hk/), which shows the scores and rankings of organizations from six Pan-Asian countries and districts (Hong Kong, Mainland China, Singapore, Macau, Malaysia, Taiwan, and Macao). The organizations in the treatment group received three bi-monthly security advisory emails in July, September, and November 2017. The treatment email includes the focal company's security performance report and a personalized URL link for the detailed information in our public website. By visiting our treatment website, the treated organizations become aware that their security performances are publicized. In addition, with the in-site search function, treatment website visitors can check other companies' security performances as well. Furthermore, we implemented tracking systems for both email and website. This enables us to precisely measure treatment effects by observing the subjects' decisions on opening emails and visiting our website. For example, we cannot expect any treatment effects on the companies who never opened our emails, or visited the website.

Our empirical results show the treatment induced a significant reduction on outbound spam volume, which is consistent with the results from He et al. (2016). In addition, we observed higher treatment effects on companies who actually opened our treatment email, and even higher effects on the organizations who proactively visited our treatment website. Interestingly, we have not observed any significant effect on the phishing website hosting behavior. This may confirm our conjecture that companies have different incentives when dealing with phishing websites.

This paper contributes to the literature in the following ways: (1) we published the first security index website in the Pan-Asian region, using the entire population of organizations in six target countries who own at least one Autonomous System Number (ASN) and valid email address, (2) based on a rigorous field experiment, we suggest an effective cyber policy designed to deal with possible internal threats from

[18] It is common for hosting companies to have 'terms and conditions' which passes security responsibilities to their customers. "You will be held responsible for all actions performed by your account whether it be done by you or by others! If server security is compromised, the account holder is responsible for all violations of the TOS and AUP, including SPAM, and all disconnect and reconnect fees associated with violations."

[19] According to Moore and Clayton (2011), Hacked server was 75.8% among all phishing websites in October 2007 - March 2008.

[20] Examples: www.icloud-com-location.tk, i.lcloud-lphone.net

[21] olympic.sinohosting.net domain appeared 86 times in our data

botnets and externality issues resulting from hosting phishing websites, and (3) by using an email tracking and web analytics tool, we are able to conduct regression analysis.

2. Literature Review

2.1 Security investment strategies

Researchers from information systems, computer science, and economics are eager to find more efficient solutions to deal with the emergence of endless cybersecurity threats. The root causes of burgeoning cybercrime are discussed from both technical and economic perspectives. The potential causes include: (i) technical vulnerabilities on the part of organizations, (ii) insufficient economic motivations to counter cybercrimes, and (iii) lack of effective legislation. Without adequate information security measures (e.g., insecure cryptographic protocols, missing anti-virus software), organizations become easy targets for security attacks (Arce 2003; Ranathunga 2014). To combat technical vulnerabilities, a number of solutions are proposed, for example, spam filtering (Bratko et al. 2006; Cormack and Lynam 2007), intrusion detection systems (Denning 1987; Lee and Stolfo 1998; Roesch 1999), and digital forensics (Casey 2011; Taylor et al. 2014). However, maintaining good information security requires significant investment (Gordon and Loeb 2002). Thus, without economic motivation, organizations are reluctant to invest in security infrastructure and countermeasures (Anderson and Moore 2006).

As cybersecurity threats are unexpected events and thus hard to predict, it is sometimes difficult to quantify the returns on investment in security adoption (Zobel and Khansa 2012; Gordon and Loeb 2002). Many organizations do not fully comprehend the threats posed by emerging, sophisticated cyberattacks and usually adopt a wait-and-see approach in security investments until a huge security incident affects them significantly (Gordon et al. 2003, Cerullo 2004). Lack of cyber security is due partially to underinvestment, which is the result of distorted incentives created by asymmetric information, network externality, and moral hazard (Anderson 2001; Bauer and van Eeten 2009). Legislation can be a good way to curb cyberattacks by heightening public awareness against cybersecurity threats (D'Arcy et al. 2009).

Existing works, such as Moore and Clayton (2011), Quarterman et al. (2013), and Tang et al. (2013), have documented that security information publication helps improve Internet security conditions at the country level. Furthermore, He et al. (2016) extended the literature by proposing an organizational-level security evaluation framework to alleviate the security information asymmetry issue. Specifically, the authors designed a policy for organizations' security information disclosures to provide more economic motivations for organizations to improve their Internet security protection. Such disclosure of information helped reduce the information asymmetry issue within organizations. Due to insufficient internal resources and policies, organizations may not have a full understanding of their security problems (D'Arcy et al. 2009). In addition, the theory of asymmetric information predicts that organizations will underinvest on cybersecurity when their customers cannot distinguish companies with strong security from those with weak security. Publicizing evaluation reports can force organizations to raise their cybersecurity awareness for the fear of losing customers to their competitors (Gal-Or and Ghose 2005; Tang et al. 2013). Furthermore, an industry-level, peer-ranking system may put peer pressure on

organizations. In this case, organizations with poor performance could face more pressure from their peers.

2.2 Studies on Cyberattacks

To evaluate organization's security levels, this research collected data on two common online scams, namely spamming and phishing. Spam usually consists of unsolicited bulk messages sent out by advertisers to promote their products. Many countries have enacted laws to prevent the spread of spam (e.g., the CAN-SPAM Act in the U.S. and UEMO in Hong Kong). However, adversaries usually use a network of compromised computers (also known as botnets) to send spam, which can make it difficult to identify the real spammers. Collecting spam data from CBL and PSBL anti-spam block lists, Quarterman et al. (2013) developed a public website, SpamRanking.net, for the spam rankings of U.S. companies.

Apart from spam, phishing is another recent online crime that poses a huge threat to financial communities. Bose and Leung (2008) conducted research to assess phishing preparedness of Hong Kong banks and compared their performance with that of their counterparts in Singapore. The study found that companies in both regions perform well when handling bogus phishing websites but need further improvement in handling phishing emails. Also, government advocacy plays an important role in encouraging organizations to adopt adequate counter-phishing security measures. Apart from government advocacy, a more in-depth study conducted by Bose and Leung (2009) finds that the antecedent factors causing firms to adopt counter-phishing measures include credit ratings, frequency of phishing attacks, and proliferation of online banking. To maintain the reputation of firms in the area of online banking, organizations tend to adopt more sophisticated anti-phishing measures to safeguard the online security of customers. Adoption of anti-phishing measures may provide a signaling effect to customers that the firms are caring and technologically advanced (Bose and Leung 2013).

Botnet is a neologism combining "robot" and "network." It refers to a collection of computer networks that are contaminated by malware (e.g., virus and Trojan) and controlled by an adversary (Stone-Gross et al. 2009). After gaining control of a network of computers, the adversary usually use botnets like a group of robots to launch various security attacks, such as spam, phishing, and denial-of-service attacks. The victims whose computers are contaminated by malware are usually unaware that their computers are being used by the adversary to launch various cyberattacks; such computers are termed zombie computers. Because an adversary uses remote zombie computers to launch cyberattacks, it is very difficult for legal authorities to catch the actual adversary or person. Furthermore, it is difficult for persecutors to collect evidence showing that the adversary launched the cyberattacks. Companies with a weak information security infrastructure have a higher chance of being attacked by malware and becoming a part of a botnet. Therefore, it is important that firms regularly check their corporate information security to ensure that it is up-to-date.

While conducting this research, we contacted and received reliable sources of data from international spam and phishing organizations. Based on the volume of spam and phishing from registered domain networks, as measured by ASNs, we developed an information security index that can reflect the security status of a company. As some firms are unaware of their security status, public disclosure of such information may help the firms better evaluate their information security infrastructure. With more

information, firms may adopt better security policies and advanced security systems. Hence, it may help firms strengthen their security over time.

3. Experimental Design and System Implementation

Hundreds of thousands of personal and business banking details are phished by fake emails and websites. Computers and servers infected with malware or viruses are turned into remotely controlled botnets to send out spam or contribute to DDoS attacks. Email continues to be a popular and effective delivery method for spam, phishing, malware, and, most recently, ransomware. Overall, the proportion of emails that include malware, viruses, or even ransomware is rising dramatically.[22] An organization's Internet security condition is a latent variable that cannot be measured directly. One way to estimate it is by using perceptible data, such as outbound malicious emails and phishing feeds. Symantec's MessageLabs published the 2016 Internet Security Threat Report, which indicates that the global spam volume per day was 24.7 billion messages with an overall email spam rate of 53% in 2015 (Symantec 2016). Among these messages, over 50% of the spam volume was sent by botnets. These infected computers and servers may be used by adversaries as a medium for even more serious cyberattacks, such as phishing, DDoS attacks, identity thefts, hacking, data breaches, and data alterations. Security attacks originating from a corporate network can be a good indicator of weak security infrastructure. In this research, we use: (1) the volume of outbound spam, and (2) real-time phishing intelligence feeds from data sources to construct a comprehensive information security indicator. A voting system Borda count method (Adelsman et al. 1977) is used to derive a composite ranking from four constituent rankings from each data source. Organizations with higher Borda counts are ranked higher, indicating a low security level. All organizations with no volume are ranked equally with the lowest rank.

3.1. Large-Scale Randomized Field Experiment

In order to causally test whether publicized security information will induce firms' awareness towards their corporate security and improve their protection level over time, we employ RFE along with econometric analysis as the main evaluation methodology. RFE, also known as a randomized controlled trial (RCT), is a well-established evaluation methodology in the social sciences for policy interventions, in which the findings can be explained by different factors associated with the interventions or the evaluation (Heckman and Smith 1995). The main advantage of this methodology is its capability of detecting a causal relationship in a naturally occurring environment.

The organizations or subjects in the experiment fall into two equally-sized, statistically homogeneous groups, which were divided with stratified and match-pair randomization (Morgan and Rubin 2012). The grouping is summarized in Figure 1. In the control group, there was no treatment. In the public group, three treatment emails were sent to relevant contacts in IT departments within each organization to inform

[22]Cisco Midyear Cybersecurity Report 2016
https://www.cisco.com/c/dam/assets/offers/pdfs/midyear-security-report-2016.pdf
Symantec Internet Security Threat Report - Email Threats 2017
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-email-threats-2017-en.pdf

the companies of their security evaluation results. Each treatment email included the organization's spam and phishing data, such as total spam mail and phishing website volume, peer rankings in the corresponding industry sectors or certain region, as well as a hyperlink to a designated webpage for the treated organization.

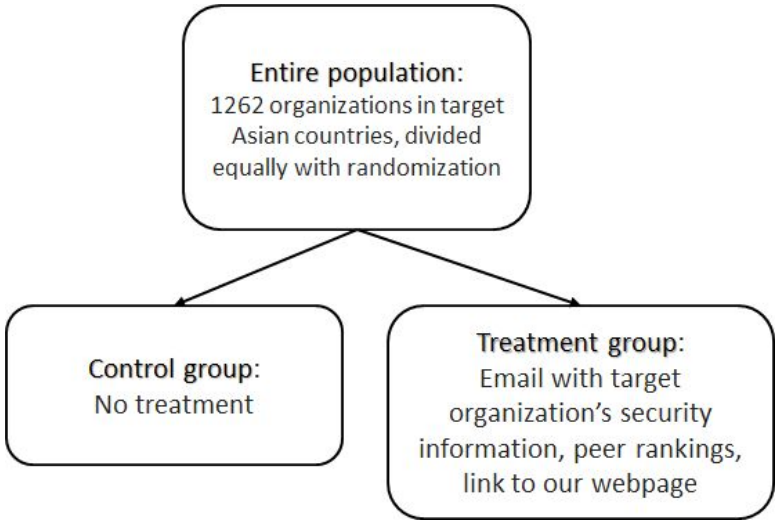

Figure 1: Design of the Randomized Field Experiment

3.2. Data

Firstly, we collected a full list of 1930 registered ASNs' information from the target countries. After mapping the ASNs to registered company names, we created a list of 1293 organizations who own at least one ASN. Lastly, we manually collected and validated corporate email addresses from those organizations, and finalized a list of 1262 organizations. It is important to point out that our field experiment was conducted with a 'full population' of organizations who own at least one registered ASN and a valid email address in six Pan-Asian countries and districts. Table 1 shows the number of companies in each country.

Figure 2 shows the architecture of the entire experiment system. The system is concurrently hosted by the Center for Research on Electronic Commerce (CREC) of the McCombs School of Business at The University of Texas at Austin and the Department of Information Systems at the City University of Hong Kong.

The system collects malicious email and website data on a daily basis from various sources: (i) spam/phishing email data from Spamhaus' Composite Blocking List (CBL) and Spamikaze's Passive Spam Block List (PSBL), and (ii) phishing website data feeds from the Anti-Phishing Working Group (APWG) and OpenPhish. CBL and APWG's daily reports are collected by the spam and phishing data collector, the Topaz server, through rsync (a Unix-based file synchronization program), while PSBL and OpenPhish real-time data feeds of the actual spam and phishing contents are stored in the Topaz server through InterNetNews (inn2). Each spam block list provides daily reports on the total spam volume associated with a complete list of spamming IP addresses. In addition, CBL provides botnet information, when available. The data cover more than eight million IP address, over 190,000 netblocks, and around

21,000 ASNs for 200 countries. PBSL has a relatively smaller daily volume compared to CBL, but it provides full email information, including raw email header, body, and attachments.

Countries and Districts	Number of Organizations	Control Group	Treatment Group
Hong Kong	309	631	631
Mainland China	309		
Singapore	264		
Malaysia	171		
Taiwan	138		
Macau	4		
Others[23]	67		
Total	1262	1262	

Table 1: Number of organizations for each country and district.

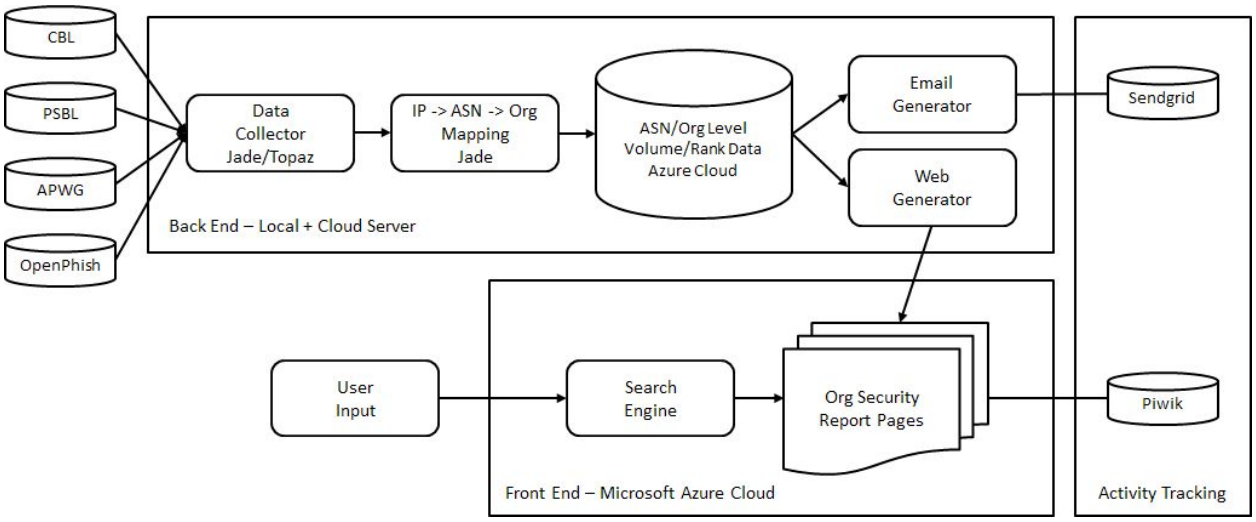

Figure 2: System Design and Implementation

The system collects malicious email and website data on a daily basis from various sources: (i) spam/phishing email data from Spamhaus' Composite Blocking List (CBL) and Spamikaze's Passive Spam Block List (PSBL), and (ii) phishing website data feeds from the Anti-Phishing Working Group (APWG) and OpenPhish. CBL and APWG's daily reports are collected by the spam and phishing data collector, the Topaz server, through rsync (a Unix-based file synchronization program), while PSBL and OpenPhish real-time data feeds of the actual spam and phishing contents are stored in the Topaz server

[23] IP addresses located in the target countries, but owned by global companies. In these cases, country codes follow the parent companies. Examples: Yahoo, Inc. owns 8 million IP addresses in Pan Asian countries.

through InterNetNews (inn2). Each spam block list provides daily reports on the total spam volume associated with a complete list of spamming IP addresses. In addition, CBL provides botnet information, when available. The data cover more than eight million IP address, over 190,000 netblocks, and around 21,000 ASNs for 200 countries. PBSL has a relatively smaller daily volume compared to CBL, but it provides full email information, including raw email header, body, and attachments.

APWG provides phishing feeds via an "eCrime Exchange service" and data feeds through a phishing data repository (e.g., open and end dates, URLs, Confidence Levels, IP addresses, etc.). OpenPhish offers free daily phishing intelligence feeds from multiple streams, and the analysis is done by applying several prominent phishing detection algorithms. The data repositories of OpenPhish include phishing URLs, targeted brands, IP addresses, country codes, ASN information, top-level domains, and discover times. In addition, using raw IP-level data, organization-level data need to be constructed in order to evaluate an organization's security conditions. Thus, there are three levels of mapping: from IP to netblock, from netblock to ASN, and, finally, from ASN to organization. With this mapping, it is possible to trace the host organization of spam mail and phishing websites.

3.3. Treatment Channels

Emails and the website, which are the two main treatment channels, play important roles in the experimental design. The email sending system was developed to compose and send advisory emails bi-monthly to the treatment group with customized organizational security reports and URL links for access to security-ranking web pages. Each security report included the past 3 months of spam volume, number of newly discovered phishing hosts, and peer rankings in the corresponding countries and industry sectors. We provided an un-subscription option for organizations which no longer wanted to receive emails. By the end of the experiment], we had received 2 un-subscription requests, and these organizations were excluded from the analysis.

In addition to the email system, a public website was created to provide organizational security reports to treated organizations and the general public. Visitors could search for organizations by name, ASN, industry code, and country or district. On the target organization's page, users could select target months from May 2015 to December 2017 and data type (combined overall, CBL, PSBL, APWG, or OpenPhish). It showed daily and monthly volumes and the rankings of firms from three dimensions, namely at the organization, industry, and country levels. The website, which is still active, is currently constructed on a Microsoft Azure platform to provide access to users in countries with limited access to the Internet due to censorship.[24]

Our website outperforms several existing sites (e.g., CBL, Spamhaus, and Cisco) from multiple perspectives:

1) It gives a more complete picture by including "smaller" spammers. In addition to the "top 10" or "top 100" spam senders, there are still a lot of organizations sending out a significant amount of spams every

[24]Microsoft Azure is the world leading cloud computing platform with service in mainland China.

day, according to the aforementioned data sources. In addition, it is possible to search for organizations which do not have outgoing spam or phishing activities.

2) It provides organizational-level information on spamming and phishing. Given that many organizations operate multiple ASNs, the metric will combine ASN-level data into organizational data.

3) Instead of snapshot data, it provides continuous and dynamic security information over a long time period from various data sources. Using the longitudinal data, users can track how an organization's security situation evolves.

4) It provides unique security ranking data sorted by industry sectors. To identify close competitors correctly, a unified, standard industry classification, such as HSIC (Hong Kong Standard Industrial Classification[25]), should be applied to all Pan-Asian countries in the sense that such a classification is modeled on the United Nations' International Standard Industrial Classification of All Economic Activities Revision 2 (ISIC Rev. 2).

3.4. Treatment response tracking

In addition to the website, email tracking and web analytics tools were deployed to check whether or not organizational representatives visited the website and became aware of their information security status. Tracking this information enabled us to perform multiple regression analyses, such as Difference-in-Difference (DID) analysis and two-stage least square analysis, as will be seen in Section 4. A powerful email management tool, Sendgrid,[26] was used to track the responses from the treatment group. It provides information on several email-related activities, including delivery, opening, and clicking. We first checked to see whether an email was successfully delivered to the target mailbox or not[27]. Once it was delivered, the system detailed information concerning email opening activity, such as the time and IP addresses used to open the email. Also, we tracked whether the internal links to websites were clicked or not. However, depending on the webmail tool, there were some cases in which an opening action was not traceable. In those cases, we used the 'click' information, which was always traceable with the unique URL link embedded in each email. Web analytics using Piwik[28] was then conducted to observe visitor behaviors on the treatment website. We tracked visitors' IP address, location, date and time, opened pages (URLs), and the duration of visits on each page. By using all available information, we then mapped visitor information to their matching organization.

4. Empirical Analysis

Our data were taken from 1,262 organizations from six Pan-Asian countries and districts: Hong Kong, Mainland China, Singapore, Macau, Malaysia, Taiwan, and Macao. Among them, 631 organizations were randomly selected for the treatment group and the rest were placed in the control group. Starting in July

[25]Hong Kong Standard Industrial Classification. https://www.censtatd.gov.hk/hkstat/un/class/hsic/index.jsp
[26] https://sendgrid.com/
[27] There are conditions which indicate delivery failure: bounced, blocked, unsubscribed
[28] Rebranded as Matomo (From January 2018), https://matomo.org

2017, we sent out a batch of security information emails to organizations in the treatment group every two months, for a total of three batches. Overall, 565 out of 631 treatment organizations successfully received at least one treatment email. As a result, we used these organizations and their corresponding control organizations as our empirical analysis data set, for a total of 1,130 organizations. Table 2 contains the summary statistics for the main variables in our analysis.

Variable	Variable description	Mean	S.D.	Max	Min
CV	CBL Volume	151661.8	2269080	1.00e8	0
PV	PSBL Volume	147.9001	2698.253	157765	0
AV	APWG Volume	0.2372	6.1761	456	0
OV	OpenPhish Volume	0.3249	3.1254	105	0
Number of IP addresses	Total number of IP addresses owned by each company	610223.4	7273093	2.33e8	0
If has social media account	If the company has at least one social media account	0.7035	0.4569	1	0
HSIC	Hong Kong Standard Industrial Classification Code			960299	50000
If has opened treatment emails	If an organization has opened a treatment email on or before this month	0.2062	0.4048	1	0
If has visited treatment website	If an organization has visited our website on or before this month	0.07080	0.2566	1	0

Table 2: Summary statistics

Variable	No control	Industry fixed effects	K-S prob (P value)
Ln CV_6	0.06324	0.05203	0.934
	(0.2123)	(0.2122)	
Ln PV_6	0.05482	0.05312	0.998
	(0.07841)	(0.08130)	
Ln OV_6	0.02460	0.02558	1.000
	(0.01978)	(0.02089)	
Ln AV_6	0.003235	0.003348	1.000
	(0.007080)	(0.007499)	
Ln_IP	-0.1309	-0.1580	0.880
	(0.2407)	(0.2483)	
If_social	5.241e-4	9.156e-4	1.000
	(0.02719)	(0.02742)	
HSIC2			1.000

Table 3: Baseline comparison for internal validity

In order to evaluate whether the security performance of the organizations in the treatment group has improved after our experimental intervention, we compare treatment organizations' outbound spam and phishing volume before and after our experiment intervention with those from the control group. Since we sent out the first batch of emails in July, we use six-month average spam and phishing volume (from Jan 2017 to June 2017) before the experiment as organizations' security measures before the experiment. To check the internal validity of our randomized field experiment, we use multiple methods to test if organizations in the treatment group are statistically equivalent to those in the control group. The results are shown in Table 3. 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.

4.1. Difference-in-Differences analysis

For the empirical analysis, we use companies' spam and phishing volume from July 2017 to December 2017 as companies' security measures after our experimental intervention. If an organization's security condition has improved, we would expect its spam and phishing volume to decrease compared with those of control group after our treatment. For the panel data set of organizations' spam and phishing information from Jan 2017 to Dec 2017, we apply a DID model to estimate the treatment effect of our email notification. In particular, the email treatment dummy variable $emailtreat_{it}$ is set equals to 1 if an organization i is in the treatment group and has successfully received the treatment email in month t. Specifically, the ordinary least squares (OLS) regression function is as follows:

$$y_{it} = \alpha_0 + \alpha_1 * emailtreat_{it} + \theta_i + \sigma_t + \epsilon_{it},$$

where y_{it} is one of the security performance measures in our data set. From Table 2, we can see that the distributions of all main variables are highly skewed, so we use log transformed spam or phishing volume as our dependent variables. Specifically, using CBL spam volume as an example, the dependent variable used in the analysis is $ln(CV) = log(CV + 0.01)$. In this function, α_1 is our main variable of interest. If α_1 is negative and statistically significant, then compared with organizations in the control group, the security performance of those in treatment group has improved after our email intervention. In order to control for organization's time-invariant unobservable characteristics and temporal variation, we also include organization-specific (θ_i) and month (σ_t) fixed effects in our regression.

The main results are reported in Table 4. We can see that, among different security performance measures, our email treatment only influences significantly organizations' outbound spam volume as measured by CBL. The estimated treatment effect for PSBL spam volume is negative but not statistically significant. On the other hand, for phishing information, there is no evidence showing that our intervention will motivate companies to reduce their phishing volume. The results support our proposition that organizations will have different responses to spam and phishing information. While organizations care about their own potential security issues, they are more reluctant to solve problems which may bring a negative impact to the rest of the world. This can be explained by the negative externality of information security (Anderson and Moore 2006).

	ln(CV)	ln(PV)	ln(AV)	ln(OV)
	(1)	(2)	(3)	(4)
Emailtreat	-0.201*	-0.0237	0.0464	0.00577
	(0.115)	(0.0659)	(0.0291)	(0.0353)
Organization fixed effects	yes	yes	yes	yes
Month fixed effects	yes	yes	yes	yes
Constant	-1.256***	-3.940***	-4.439***	-4.350***
	(0.0570)	(0.0355)	(0.0187)	(0.0206)
Number of observations	13,560	13,560	13,560	13,560
Number of organizations	1,130	1,130	1,130	1,130

Note: Clustered standard errors in brackets *** p<0.01, ** p<0.05, * p<0.1

Table 4: DID analysis on monthly security measures

4.2 Heterogeneous treatment effects

One possible reason of the insignificant results is that many organizations did not have positive spam or phishing volumes during the period of our experiment. As security condition is a relatively hard characteristic to observe, our existing security measures could not evaluate all organizations' cyber security conditions in a very accurate way. Though these organizations' security protection levels may have changed, we may lack the ability to precisely measure the difference in our current experiment. Please see detailed numbers in Table 5. Approximately 40% of all organizations in our data set showed positive spam volume based on CBL. However, only about 22% of them had positive spam volume based on PSBL. For the two phishing volume measures, only approximately 5% and 8% of organizations had positive volume based on APWG and Openphish respectively.

	Number of orgs	Number of orgs with positive volume before experiment (treatment)	Number of orgs with positive volume before experiment (control)
CV	1130	228	230
PV	1130	131	120
AV	1130	31	27
OV	1130	46	43

Table 5: Number of organizations in control and treatment groups with positive spam or phishing volume

For the reasons mentioned above, we add an interaction term between the $emailtreat_{it}$ and the dummy variable which indicates whether companies have positive spam or phishing volume before the experiment. If our treatment emails are effective, we should observe that spam or phishing volume from

those organizations with positive numbers have a larger reduction after the beginning of the experiment. The OLS regression function is displayed below:

$$y_{it} = \beta_0 + \beta_1 * emailtreat_{it} + \beta_2 * emailtreat_{it} * positive_i + \rho_i + \tau_t + \epsilon_{it},$$

where $positive_i$ indicates whether organization i has positive number of one particular security measure. The results are reported in Table 5. Compared with the data in Table 3, we find that the magnitude of the treatment effect for CBL spam volume is larger. More importantly, the treatment effect for PSBL spam volume is significantly negative and the magnitude is very close to that of CBL. This further indicates that our email treatment will motivate organizations to improve their security protection, leading to less outbound spam volume. However, for the phishing performance, we still could not find evidence of a reduction in phishing volume. One reason may be the small number of data points in the analysis.

	CV (log)	PV (log)	AV (log)	OV (log)
	(1)	(2)	(3)	(4)
Emailtreat	0.251***	0.306***	-0.0118	0.0468**
	(0.0879)	(0.0511)	(0.0215)	(0.0211)
Emailtreat*Positive	-1.118***	-1.420***	1.057***	-0.502
	(0.207)	(0.162)	(0.327)	(0.354)
Organization fixed effects	yes	yes	yes	yes
Month fixed effects	yes	yes	yes	yes
Constant	-1.256***	-3.940***	-4.439***	-4.350***
	(0.0574)	(0.0374)	(0.0197)	(0.0204)
Observations	13,560	13,560	13,560	13,560
Number of organizations	1,130	1,130	1,130	1,130

Note: Clustered standard errors in brackets *** p<0.01, ** p<0.05, * p<0.1

Table 6: Heterogeneous treatment effect analysis for organizations with and without positive security measures before the experiment.

4.3 Two-stage least squares analysis

One potential reason for the relatively weak treatment effect is that employees of these treated organizations may not actually think over our emails. For example, the successfully delivered emails may not be opened at all. On the other hand, some organizations may pay more attention to our treatment by visiting our website through the link in the email.

Table 7 shows the organizations' responses to our treatment gathered by the email tracking (Sendgrid) and web analytics (Piwik) tools. In the table, the treatment group is divided into two subgroups, based on spam and phishing records in 2017. Among 565 organizations who successfully received our treatment emails, 257 (45.5%) had emitted at least one spam email or hosted at least one phishing website. The email opening data showed that 6% more organizations who had zero volume endogenously decided to open the email titled "Security Advisory Report for (organization name)," sent from email address "advisory@cityu.edu.hk." It tells us that organizations who have better protection care more about

security-related news (Z-score = 1.4011, p-value = 0.08076, one-tailed). However, once the email was opened, website visit rates and multiple visit rates are nearly identical within the minimal error rate (1) between the two groups.

Volume from all data sources	Number of organizations in the treatment group			
	Total	Opened Email (/Total)	Visited website (/Open)	Multiple Visits (/Visit)
Orgs with no spam and phishing	308	150 (48.7%)	44 (29.3%)	33 (75.0%)
Orgs with 1+ spam or phishing	257	110 (42.8%)	32 (29.0%)	25 (78.1%)
Total	565	260 (46.0%)	76 (29.2%)	58 (76.3%)

Table 7: Email open/website visit counts among 565 companies who received our treatment email.

	ln(CV)	ln(PV)	ln(AV)	ln(OV)
	(1)	(2)	(3)	(4)
Open a treatment email	-0.591*	-0.165	0.120	0.00636
	(0.346)	(0.190)	(0.0874)	(0.104)
Organization fixed effects	yes	yes	yes	yes
Month fixed effects	yes	yes	yes	yes
Constant	-1.256***	-3.940***	-4.439***	-4.350***
	(0.0570)	(0.0355)	(0.0187)	(0.0206)
Number of observations	13,560	13,560	13,560	13,560
Number of organizations	1,130	1,130	1,130	1,130

Note: Clustered standard errors in brackets *** p<0.01, ** p<0.05, * p<0.1

Table 8: 2SLS for treatment effects on opening treatment emails

One econometric challenge of estimating these treatment effects is that these actions, including opening emails and visiting websites, are endogenously determined by treated organizations. Estimating directly the regressions with corresponding dummy variables may lead to biased estimators. Taking advantage of our randomization, we use the dummy variable indicating whether or not the security measure is from a treatment organization after July 2017 as an instrumental variable (IV) for an organization's decision to open an email or to visit our website. Since only organizations in the treatment groups can receive our treatment emails, the monotonicity condition is satisfied in our case. Then we apply two-stage least square regression (2SLS) to estimate the local average treatment effects of opening our email and visiting our website (Imbens and Angrist, 1994). The specific regression functions are as follows:

$$D_{it}^{*} = \gamma_0 + \gamma_1 * emailtreat_{it} + \epsilon_{it},$$

with the observed email opening or website visiting indicator, D_{it} related to the unobserved latent index, D_{it}^{*}, by

$$D_{it} = \begin{cases} 1, & D_{it}^{*} > 0 \\ 0, & D_{it}^{*} \leq 0. \end{cases}$$

Further, the dependent variable y_{it} is related to the treatment by the equation

$$y_{it} = \beta_0 + \beta_1 D_{it} + \mu_{it}$$

The results for the local average treatment effect of opening an email and visiting our website are reported in Tables 8 and 9. All the standard deviations are robust and clustered at a company level. Similar to the results in Table 4, only the coefficient of companies' spam volume based on CBL is negative and significant. However, the magnitude of the coefficient is much larger (-0.591 and -1.931), indicating that organizations who indeed opened the emails and visited our website tend to perform better. More specifically, outbound spam volume from organizations which opened our emails decreased by 44.1% and that from organizations which visited our website is reduced by approximately 85.4%. There are two potential mechanisms which can be used to explain our results: 1. only organizations which opened our treatment emails received our treatment, leading to enhanced security performance; and 2. organizations who chose to open our emails or even visited our websites are those who are more vigilant about potential security threats. Hence, they are more likely to improve their security safety measures after receiving our treatment emails.

	ln(CV)	ln(PV)	ln(AV)	ln(OV)
	(1)	(2)	(3)	(4)
Visit treatment website	-1.931*	-0.539	0.392	0.0208
	(1.141)	(0.624)	(0.290)	(0.340)
Organization fixed effects	yes	yes	yes	yes
Month fixed effects	yes	yes	yes	yes
Constant	-1.256***	-3.940***	-4.439***	-4.350***
	(0.0572)	(0.0355)	(0.0187)	(0.0206)
Number of observations	13,560	13,560	13,560	13,560
Number of organizations	1,130	1,130	1,130	1,130

Note: Clustered standard errors in brackets *** p<0.01, ** p<0.05, * p<0.1

Table 9: 2SLS for treatment effects on visiting our website

Similarly, we applied 2SLS to investigate if the treatment effects of opening treatment emails and visiting treatment website are more significant for organizations with observed security issues before the experiment. Please find the corresponding estimators in Tables 10 and 11. Again, we find the estimated treatment effects are larger for opening an email or visiting our website compared with those for receiving our emails. These empirical results further support our conclusion that our email treatment will lead to less spam volume for organizations with observed security issues. One interesting result is that, for spam volume measured based on PV, we do observe significant volume reduction, which is another empirical piece of evidence showing the effectiveness of our treatments. Hence, the insignificant results in the main results for the PV may due to the fact that many organizations do not have positive outbound spam

volume in the first place. Another interesting finding is that for phishing volume based on OV, though the magnitudes are quite large, the estimated treatment effects are not statistically significant.

In summary, based on our empirical analysis results, we find statistically significant spam volume reduction for treated organizations in our experiment compared with control organizations. On the other hand, we did not observe a significant change in organizations' phishing performance during the experiment. The results may indicate that organizations have different incentives regarding spam emission versus phishing hostings. Essentially, our phishing measure evaluates the number of phishing websites hosted by the focal firm, and the websites are targeting external entities. In that sense, this is an externality issue where the associated risk does not directly harm the focal organization. For the hosting service providers, phishing website owners can be considered as legitimate customers. As a result, organizations may not have a strong incentive to take down the questionable websites. We argue that regulations or policies should take in place to internalize the costs and risks these organizations bring to other counterparties.

	ln(CV)	ln(PV)	ln(AV)	ln(OV)
	(1)	(2)	(3)	(4)
Open a treatment email	0.545***	0.223***	0.123***	0.0614**
	(0.126)	(0.0757)	(0.0343)	(0.0302)
Open*Positive	-3.395***	-5.515**	2.874	-2.405
	(0.786)	(2.617)	(1.843)	(2.132)
Organization fixed effects	yes	yes	yes	yes
Month fixed effects	yes	yes	yes	yes
Number of observations	13,560	13,560	13,560	13,560
Number of organizations	1,130	1,130	1,130	1,130

Note: Clustered standard errors in brackets *** p<0.01, ** p<0.05, * p<0.1

Table 10: 2SLS for heterogeneous treatment effects on opening treatment emails

	ln(CV)	ln(PV)	ln(AV)	ln(OV)
	(1)	(2)	(3)	(4)
Visit treatment website	1.737***	0.700***	0.394***	0.203**
	(0.447)	(0.242)	(0.115)	(0.102)
Visit*Positive	-3.360***	-5.469**	2.911	-2.421
	(0.800)	(2.628)	(1.851)	(2.135)
Organization fixed effects	yes	yes	yes	yes
Month fixed effects	yes	yes	yes	yes
Number of observations	13,560	13,560	13,560	13,560
Number of organizations	1,130	1,130	1,130	1,130

Note: Clustered standard errors in brackets *** p<0.01, ** p<0.05, * p<0.1

Table 11: 2SLS for heterogeneous treatment effects on visiting our website

5. Discussion and Concluding Remarks

Using a large-scale randomized field experiment, we empirically study how security evaluation publication affects organizational security levels in Pan-Asian countries and districts. To measure the pre- and post-experimental information security risk level of the organizations, we use two distinct perceptible cyberattack data: outbound spam volume and phishing websites. To increase security awareness in the general public and increase economic motivations on the part of organizations, security performance rankings were published on our project website. In doing so, an organization with a weak information security level may have faced a threat of reputation loss among customers. From a series of regression analysis on two different types of security attacks, we found evidence that the security report publication has a statistically significant effect in reducing spam volume. The treatment effects gradually increased from receiving emails (results from DID) to opening emails and visiting the website (results from 2SLS).

On the other hand, we do not find a statistically significant effect on phishing website hosting behavior. There are two possible explanations for this: First, web hosting companies do not have economic incentives to eliminate phishing websites as they are legitimate customers of the hosting services. This can be considered to be a negative externality issue. Second, there is a lack of strict phishing-related policies in Pan-Asia compared to those geared toward spamming activities (Appendix 1), and those in force impose less liability risk for the website hosting services. Following this line, some ISPs and hosting services have policies which pass responsibilities on to their customers. Although we did not have statistically significant results in phishing reduction, we observed anecdotal cases in which our treatment induced positive changes: among 46 treated companies who hosted phishing websites according to OpenPhish data, six of them actually eliminated all phishing websites within one or two months after their first response (opened an email and/or visited the website) to our treatment. Based on the other phishing data from APWG, among 31 organizations hosting phishing websites, four addressed the issues fully. This may suggest that the provided information was appreciated and induced a certain level of improvement in the subject's security protection level. To summarize, our results from the empirical analysis suggest that security monitoring websites, such as cybeRatings, can be effective in terms of reducing botnet activities represented by outgoing spam volume. At the same time, we observed that organizations have different incentives in terms of managing phishing attacks. This has a policy implication in that stronger regulations may be needed to internalize the negative externalities resulting from organizations hosting phishing websites.

As a functional direction, we are currently preparing multiple extensions of our experiment in terms of communication channels and scope. First, we will use massive social media platforms (e.g., Twitter, Facebook, Weibo, and WeChat) to share the security reports with the treated organizations. One unique advantage of using a social media treatment compared to an email treatment is that social media are closely followed by customers and strategic partners. As such, information disclosure on social media may lead to more pronounced reactions from the treatment organizations. In addition, by using direct messages in social media channels, deliverability could be improved from the relatively low email opening rate (46%). In order to avoid some spillover effects to the control group, the treatment effect on social media will only be applied to the public treatment group. The effect of social media treatment can

be measured by the difference between organizations who only received treatment emails and those whose security reports are also disseminated via social media.

The second extension is to expand the scope of the experiment. Organizations' preparedness in terms of cybercrimes has become a global debate in this globally hyper-connected economy. It is also possible that the designs or regulations that are effective in the U.S. or Pan-Asia may not work on other continents (Kugler 2015). As cybersecurity issues are not isolated to specific countries, it is necessary and beneficial for all countries to collaborate on this issue. As our spam and phishing data include information from more than 200 countries worldwide, we plan to generate and publicize security reports for other countries' organizations. Doing so will increase the population size of the experiment, which was a limitation for our study in Asia. With a larger sample size, we plan to add more treatment groups with different email contents. For example, one group will receive emails with general spam/phishing activity information that are similar to those used in the current study, and the other group will receive more comprehensive information, including information on the actual botnets installed in the subjects' system, possible threats from the botnets, a detailed list of IP addresses involved in the cybercrime, and possible measures to mitigate the issue.

Acknowledgement

The work described in this paper was fully supported by grants from US National Science Foundation (NSF Award Number: 1718360) and the Public Policy Research Funding Scheme (Project Number: 2015.A1.030.16A) from the Policy Innovation and Coordination Office of the Hong Kong Special Administrative Region Government.

Reference

Adelsman, R. M., and Whinston, A. B. 1977. "Sophisticated Voting with Information for Two Voting Functions, " Journal of Economic Theory (15:1), pp. 145-159.

Anderson, R. 2001. "Why Information Security Is Hard - an Economic Perspective," Proceedings of 17th Annual Computer Security Applications Conference, 2001. ACSAC 2001. , pp. 358-365.

Anderson, R., and Moore, T. 2006. "The Economics of Information Security," Science (314:5799), pp. 610-613.

Arce, I. 2003. "The Weakest Link Revisited [Information Security]", IEEE Security & Privacy (1:2), pp. 72-76.

Bauer, J. M., and van Eeten, M. J. G. 2009. "Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options," Telecommunications Policy (33:10–11), pp. 706-719.

Bose, I., and Leung, A. C. M. 2007. “Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities,” Communications of the Association for Information Systems (19), pp. 544-566.

Bose, I., and Leung, A. C. M. 2008. “Assessing Anti-Phishing Preparedness: A Study of Online Banks in Hong Kong, ” Decision Support Systems (45:4), pp. 897-912.

Bose, I., and Leung, A. C. M. 2009. “What Drives the Adoption of Anti-Phishing Measures by Hong Kong Banks?, ” Communications of the ACM (52:8), pp. 141-143.

Bose, I., and Leung, A. C. M. 2013. “The Impact of Adoption of Identity Theft Countermeasures on Firm Value, ” Decision Support Systems (55:3), pp. 753-763.

Bratko, A., Cormack, G. V., Filipic B., Lynam, T. R., and Zupan, B. 2006. “Spam Filtering using statistical data compression methods.” Journal of Machine Learning Research 6: pp. 2673-2698.

Carl, G., Kesidis, G., Brooks, R. R., and Rai, S. 2006. "Denial-of-service attack-detection techniques." IEEE Internet Computing (10:1), pp. 82-89.

Casey, E. 2011. “Digital evidence and computer crime: Forensic science, computers and the Internet. ” Academic Press.

Cerullo, V., and Cerullo, M. J. 2004. “Business Continuity Planning: A Comprehensive Approach, ” Information Systems Management (21:3), pp. 70-78.

Cormack, G. V., and Lynam, T. R. 2007. “Online supervised spam Filter evaluation.” ACM Transaction on Information Systems, Vol. 25(3), pp.11.

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

Denning, D. E. 1987. “An intrusion-detection model.” IEEE Transactions on Software Engineering, Vol. 13(2), pp. 222-232.

Gal-Or, E., and Ghose, A. 2005. “The economic incentives for sharing security information.” Information Systems Research 16(2), pp. 186-208.

Gordon, L. A., and Loeb, M. P. 2002. "The Economics of Information Security Investment, ” ACM Transactions on Information and System Security (5:4), pp. 438-457.

Gordon, L. A., Loeb, M. P., and Lucyshyn, W. 2003. “Information Security Expenditures and Real Options: A Wait-and-See Approach,” Computer Security Journal (19:2), pp.1-7.

He, S., Lee, G. M., Quarterman, J. S., and Whinston, A. B. 2015. “Cybersecurity Policies Design and Evaluation: Evidence from a Large-Scale Randomised Field Experiment, ” Proceedings of Workshop on the Economics of Information Security, pp. 1-50.

He, S., Lee, G. M., Han S., Whinston, A. B., 2016. “How Would Information Disclosure Influence Organizations' Outbound Spam Volume? Evidence from a Field Experiment,” Journal of Cybersecurity 2(1), 99-118.

Heckman, J. J., and Smith, J. A. 1995. “Assessing the Case for Social Experiments,” Journal of Economic Perspectives (9:2), pp. 85-110.

Imbens, G. W. and Angrist, J. D., 1994. “Identification and Estimation of Local Average Treatment Effects.” Econometrica, 62(2), pp.467-475.

Lee, W. and Stolfo, S. J. 1998. “Data mining approaches for intrusion detection.” Proceedings of 7th USENIX Security Symposium.

Moore, T., Clayton, R., and Anderson, R. 2009. "The Economics of Online Crime." Journal of Economic Perspectives, 23(3): 3-20.

Moore, T. and Clayton, R. 2011. “The Impact of Public Information on Phishing Attack and Defense.” Communications & Strategies (81), pp.45-68.

Morgan, K. L., Rubin, D. B. 2012. “Rerandomization to improve covariate balance in experiments.” Ann Stat 2012;40:1263–82

Quarterman, J. S., Linden, L., Tang, Q., Lee, G. M., and Whinston, A. B. 2013. “Spam and Botnet Reputation Randomised Control Trials and Policy,” Proceedings of the 41st Research Conference on Communication, Information and Internet Policy, pp. 1-13.

Rao, J. M., and Reiley, D. H. 2012. “The Economics of Spam,” Journal of Economic Perspectives (26:3), pp. 87-110.

Roesch, M. (1999). “SNORT: Lightweight intrusion detection for networks.” Proceedings of 13th Large Installation System Administration Conference, pp. 229-238.

Ranathunga, D., Roughan, M., Nguyen, H., Kernick, P. and Falkner, N., 2016. Case studies of scada firewall configurations and the implications for best practices. *IEEE Transactions on Network and Service Management*, *13*(4), pp.871-884.

Shetty, N., Schwartz, G., Walrand, J. 2010. “Can Competitive Insurers Improve Network Security?,” In: Acquisti, A., Smith, S.W., Sadeghi, A.-R. (eds.) TRUST 2010. LNCS, vol. 6101, pp. 308–322. Springer, Heidelberg.

Stone-Gross, Brett, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. “Your botnet is my botnet: analysis of a botnet takeover.” In Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 635-647. ACM, 2009.

Tang, Q., Linden, L., Quarterman, J. S., and Whinston, A. B. 2013. “Improving Internet Security through Social Information and Social Comparison: A Field Quasi-Experiment,” Workshop on Economics of Information Security.

Taylor, R. W., Fritsch, E. J., and Liederbach, J. 2014. “Digital crime and digital terrorism,” Prentice Hall Press.

van Eeten, M., Bauer, J. 2007. “The economics of malware: security decisions, incentives and externalities,” Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, DSTI/ICCP/REG, 27, Paris, OECD (2007)

Zobel, C. W., and Khansa, L. 2012. “Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks,” Decision Sciences (43:4), pp. 687-710.

Appendix 1: Cybercrime Legislation in Pan Asia

Panel A: Legislation on Spam

Country	Ordinance	Description
Hong Kong	Unsolicited Electronic Messages Ordinance (Cap 593.)[29] (2013).	Establishes rules for sending commercial electronic messages including SMS, pre-recorded messages and spam emails. Thus, serving as anti-spam legislation
Mainland China	Regulations on Internet email Services 2006	Explicitly defines a checklist for e-mail or other forms of communications sent to residents of the mainland or those residing in the Mainland.
Taiwan	Abusing Commercial Electronic Mail Management Act[30] (2012)	Specifically enacted for the purposes of maintaining the convenient use of the Internet, minimizing harassment resulting from abusing commercial electronic mail, and enhancing the security and efficiency of the Internet environment.
Pakistan	Prevention of Electronic Crimes Act 2006-Article 22 is directly related to Spam[31]	Controls for spam, which is defined as the transmission of harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain.
Singapore	Spam Control Act -Chapter 311A (Act 21 of 2007)[32]	Provides for the control of spam, which is unsolicited commercial communications sent in bulk by electronic mail or by text or multimedia messaging to mobile telephone numbers, and to provide for matters connected therewith.
Malaysia	Communications and multimedia act of 1998-section 233[33]	Controls for spam, which is defined as a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address

[29] http://www.ofca.gov.hk/filemanager/ofca/common/uemo/regulatory_framework/cop20131129.pdf

[30] http://antispam.ncc.gov.tw/english/HTML/Draft_of_Spam_Act_2012.htm#_Toc227482329 (Access date: 14/02/2018)

[31] http://www.na.gov.pk/uploads/documents/1470910659_707.pdf (Access date: 14/02/2018)

[32] https://sso.agc.gov.sg/Act/SCA2007?ViewType=Pdf&_=00010101000000 (Access date: 14/02/2018)

[33] https://www.unodc.org/res/cld/document/mys/communications_and_multimedia_act_html/Malaysia_Communications_and_Multimedia_Act_1998.pdf (Access date: 14/02/2018)

South Korea [34]	Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001- Article 50	Broad act, that covers several topics closely related to spam including, advertising, collection of e-mail addresses and malware.
Japan	Act on Regulation of Transmission of Specified Electronic Mail (2009)	Provides for proper transmission of Specified Electronic Mails, to prepare a preferable environment for the use of Electronic Mails, and thereby to contribute to the sound development of an advanced information and communications society.

[34] https://iapp.org/media/pdf/knowledge_center/S-Korea_IC_Network_Act.pdf (Access date: 14/02/2018)

Panel B: Legislation on Phishing

Country	Ordinance	Description
Hong Kong	N/A	No explicit laws
South Korea	Criminal Law-Article 347-2 (Fraud by The Use of Computer, etc.)[35]	Provides legislation against the acquisition of any benefits to property by making any data processed after inputting false information or improper order, or inputting or altering the data without any authority into the data processor, such as computers.
Indonesia	The Electronic Transaction and Information Law-Article 35 (2008)	Provides legislation against the unlawful manipulation, creation, alteration, deletion or tampering of electronic information and/or electronic documents with the intention that such electronic information and/or documents would seem to be authentic data.
Japan	Act on Prohibition of Unauthorized computer access-Article 4 &6[36] (1999)	Provides legislation against the act of rendering a specified computer with an access control feature available for specified use that is subject to restrictions imposed by the access control feature concerned, by inputting someone else's identification code associated with the access control feature concerned via a telecommunications link and thus operating the specified computer concerned.
Singapore	Access with intent to commit or facilitate commission of offence (The Computer misuse and cybersecurity act subsection 4)[7]	Provides legislation against securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence.
Malaysia	Computer crime act-Part 2, subsections 3 & 4[37]	Provides legislation against the unauthorized access to any program or data held in any computer system.

[35] http://www.wipo.int/edocs/lexdocs/laws/en/kr/kr033en.pdf (Access date: 14/02/2018)
[36] https://www.npa.go.jp/cyber/english/legislation/uca_Tentative.pdf (Access date: 14/02/2018)
[37] http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20563.pdf
(Access date: 14/02/2018)