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

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

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

Abstract

This paper investigates how the disclosure of a security vulnerability index based on outgoing spams and phishing website hosting, which may serve as an indicator of a firm's inadequate security controls, affects companies' security protection strategy. Our core objective is to study whether firms improve their security when they become aware of their vulnerabilities and such information is publicized. To achieve this goal, we conduct a randomized field experiment on 1,262 firms in six Pan-Asian countries and regions. For the treatment group of 631 firms, we alert them of their security vulnerability index and ranking over time, and their relative performance compared to their peers via emails and a public advisory website. Compared with the control group without being informed of their security vulnerability index, the treatment group improved their security over time, with a significant reduction of outgoing spam volume. A marginally significant improvement in reducing phishing hosting websites is also observed among non-web hosting firms in the treatment group. The security improvement may be attributed to firms' proactive reaction to the security vulnerability information. Our study provides cybersecurity policy makers with useful insights on how to motivate firms to adopt better security measures.

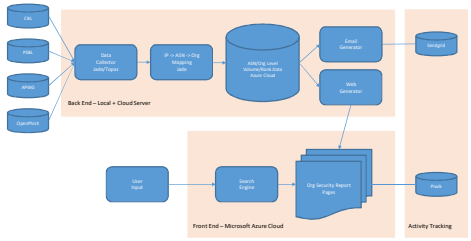
Research Question

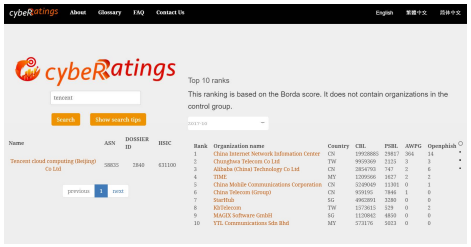
- Information Disclosure Policy
- Evaluate organizations' security level by monitoring Outgoing Attack Activity in Asia.
  - Indicator of compromised computer / network
- Comprehensive security measure
  - Help customers and investors evaluate potential information security risks of the organizations of interests
  - Encourage firms to recognize the problem and react
- Will information security awareness lead to an increase defense level against cybercrime?

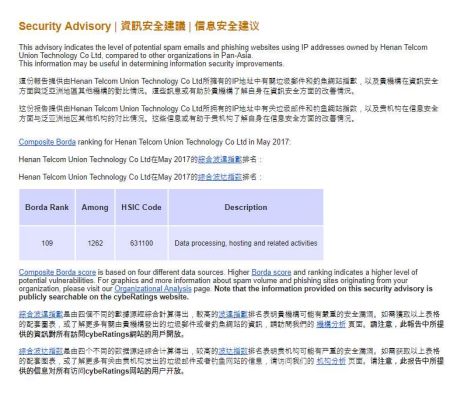
Data

- Spam
  - CBL - Composite Blocking List
    - IP, owner, Botnet
  - PSBL - Passive Spam Block List
    - IP, contents, volume, ASN
- Phishing (websites)
  - APWG - Anti Phishing Working Group
    - Biggest phishing database.
  - OpenPhish
    - Automated phishing detection.

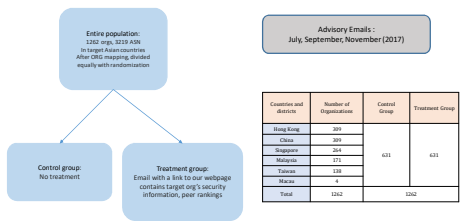
System Implementation







Randomized Field Experiment



Advisory Emails :
July, September, November (2017)

Countries and districts	Number of Organizations	Control Group	Treatment Group
Hong Kong	309	631	631
China	309		
Singapore	264		
Malaysia	171		
Taiwan	138		
Macau	4		
Total	1262	1262	

Empirical Model

- DID model
  - Random treatment
  - Monthly data in 2017
  - Org and time fixed effects
- Regressions

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

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 1: Summary statistics

Results

	ln(CV)	ln(PV)	ln(AV)	ln(OV)
	(1)	(2)	(3)	(4)
email_treat	-0.135**	-0.000842	0.00974	-0.00766
	(0.0682)	(0.0338)	(0.0114)	(0.0121)
Organization fixed effects	yes	yes	yes	yes
Month fixed effects	yes	yes	yes	yes
Constant	1.893***	0.287***	0.0417***	0.0779***
	(0.0341)	(0.0166)	(0.00522)	(0.00698)
Number of observations	13,560	13,560	13,560	13,560
Number of organizations	1,130	1,130	1,130	1,130
R-squared	0.014	0.053	0.012	0.004

Table 2: Treatment effects on different security measures

	Sample of positive spam volume		Sample with phishing websites	
	ln(CV)	ln(PV)	ln(AV)	ln(OV)
	(1)	(2)	(3)	(4)
email_treat	-0.430***	-0.128*	0.178*	-0.138
	(0.138)	(0.0708)	(0.107)	(0.120)
Organization fixed effects	yes	yes	yes	yes
Month fixed effects	yes	yes	yes	yes
Constant	3.255***	0.538***	0.335***	0.697***
	(0.0700)	(0.0340)	(0.0471)	(0.0697)
Observations	5,544	5,544	1,200	1,200
Number of organizations	462	462	100	100
R-squared	0.033	0.091	0.109	0.038

Table 3:Analysison subset firms with positive security measures before the experiment

	Full sample		Sample w/ security incidents	
	Country rank	Industry rank	Country rank	Industry rank
	(1)	(2)	(3)	(4)
email_treat	0.563**	0.177	1.304**	0.447
	(0.276)	(0.231)	(0.532)	(0.459)
Organization fixed effects	yes	yes	yes	yes
Month fixed effects	yes	yes	yes	yes
Constant	35.44***	22.59***	33.74***	22.68***
	(0.181)	(0.144)	(0.313)	(0.255)
Observations	13,560	13,560	5,472	5,472
Number of organizations	0.261	0.135	0.153	0.071
R-squared	1,130	1,130	456	456

Table 4: Treatment effects on organizations' security rankings

- Hosting and Non-hosting Firms' Phishing Websites
  - Externality issue
  - Web hosting firms might not have a strong incentive to take down phishing websites
  - Divide 124 organizations with positive phishing data into two groups
  - Find marginal significant phishing reduction for non-hosting organizations

Conclusion and Future Direction

- To summarize, our results from the empirical analysis suggest that information security monitoring websites, such as cybeRatings, can be effective in reducing botnet activities represented by outgoing spam volume.
- Meanwhile, we observed that firms have different incentives in terms of managing phishing attacks.
- This work may have policy implications in that stronger regulations may be required to internalize the negative externalities resulting from phishing websites hosted by malicious entities.
- Future direction:
  - Machine learning models to show the relationship between spam/phishing information and the probability of a data breach
  - Combining randomized field experiment with machine learning models

Acknowledgement

- Supported by US National Science Foundation (NSF Award Number: 1718360, NSF Student Travel Grant) 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.