Do Reputational Sanctions Deter Negligence in Information Security Management? A Field Quasi-Experiment

Kaoruko Kawamoto

Keio University

July 3, 2023

Thesis Information

- Title:Do Reputational Sanctions Deter Negligence in Information Security Management? A Field Quasi-Experiment
- Author : Qian Tang, Andrew B. Whinston
- Date: Accepted February 2020
- Journal: Production and Operations Management. 29, (2), 410-427

Abstract

- S ecurity negligence, a major cause of data breaches, occurs when an organization ’ s information technology management fails to adequately address security vulnerabilities.

- publicly. We find that because of our reputational sanction mechanism, organizations in the four countries, including those that were not listed, reduced outgoing spam significantly compared to those in similar countries.

- Moreover, we find that reputational sanctions have a stronger effect on large organizations and important organizations that provide network access and transit to others.

Contents

1 Introduction

- Under the reputational sanction mechanism, firms ' security practices are publicized and sanctions are imposed on firms with discovered persistent vulnerabilities, which have a direct impact on their security management reputations.

- reputation sanctions can, in effect, lead to additional sanctions by supply chain partners. From this perspective, the reputational sanction mechanism can be a cost-effective way to monitor and manage firms and their supply chain partners.

- Combating spam has great implications for reducing IT costs, increasing productivity, optimizing resource utilization, and enhancing operation resilience.

2 Literature Review

- This mechanism is powerful and effective in deterring deviant behavior and attaining social control in private markets.
- The extant literature has addressed security issues from various perspectives of software vendors, end computer users, organizations, and supply chains.
- In operations management research, theoretical studies have proposed interorganization mechanisms such as information sharing ,cost-sharing contracts,security service outsourcing and liability to mitigate security risks among the organizations within a supply chain.

3 Research Context Dataset and Method

- Composite Blocking List (CBL) and the Passive Spam Block List (PSBL), shared with us their internal daily datasets of detected outgoing spam on a daily basis
- An AS is a collection of routers with prefixes and routing policies under the administrative control of the same network service provider
- we selected the United States, Canada, Belgium, and Turkey as the four treatment countries to experiment with a reputational sanction mechanism.
- For each treatment country, we impose reputational sanctions on the top-10 ASes that send out the most spam.
- To impose actual reputational sanctions on the top-10 ASes, we then designed a website to publicly list them for each treatment country.

4.1. Quasi-Experimental Design

SCM

we consider only four treatment countries, comparing the ASes of these countries to those of other countries can be problematic due to the endogeneity issue of the country-level treatment. Therefore, we employ the synthetic control method (SCM) to construct a synthetic comparison country for each treatment country.

- the SCM compares the outcome variable of a treated country to a weighted average of the outcomes of potential controls
- First, it balances both cross-sectional and longitudinal trends to create control countries that look as similar as possible to the treated countries during the pretreatment period
- Second, it tackles endogeneity due to omitted variables by accounting for the presence of time-varying unobservable confounders.

4.2 Estimation and Results

After the SCM, the monthly data on outgoing spam volumes of the ASes within the treated and the synthetic control countries from January 2011 to March 2013 are used to estimate the effect of the country-level treatment.

- Difference-in-differences (DID) estimation has been widely used to estimate the causal effect of policy interventions in both experimental and observational studies.
- we use a fixed effects (FE) negative binomial (NB) regression model, which is commonly used if there is significant skewness in the data and a large number of zeros in the dependent variable.

4.2 Estimation and Results

Table 2 FENB Estimation of the Treatment Effect on Not-Listed ASes

	(1) All treated and synthetic controls	(2) US and synthetic US	(3) CA and synthetic CA	(4) BE and synthetic BE	(5) TR and synthetic TR	(6) Treated countries only
D_{ct}	−0.303***	−0.317***	−0.124***	−0.029	−0.332***	−0.306***
	(0.008)	(0.008)	(0.035)	(0.181)	(0.092)	(0.034)
Time FE	Yes	Yes	Yes	Yes	Yes	Yes
AS FE	Yes	Yes	Yes	Yes	Yes	Yes
No. of ASes	15,496	5970	792	9561	330	5778
No. of observations	433,888	167,160	22,176	267,708	9240	161,784

Note: Standard errors are shown in parentheses. ***$p < 0.001$, **$p < 0.01$, *$p < 0.05$.

- Table 2 reports the estimation results of the treatment effect on the not-listed ASes by using the FENB model.
- Quantitatively, our result suggests a 26.1 percents reduction in the expected outgoing spam volume on average.

4.3 Robustness Checks

The FENB model assumes that the monthly AS spam volume is independent over time, conditional on the AS fixed effects, time-specific effects and the treatment condition.

$$Y_i ct = w_i + v_i + \delta D_c t + \gamma \Gamma + \epsilon_i ct$$

$Y_i ct$ is the log-transformed spam volume, and $Y_i c, t_1$ is included as an additional control variable. Note that $Y_i c, t_1$ is likely to be endogenous because of its correlation with $\epsilon_i ct$.

- The treatment effect cannot be explained by botnet takedowns.
- The treatment effect on not-listed ASes that intentionally spam is non-negative.

Conclusion

- Quantitatively, the country-level treatment effect can reduce the expected outgoing spam volume by 26.1 percents on average for the ASes within the country, while the AS-level treatment effect leads to an additional 45.2 percents average reduction among the listed ASes.

- We also find that reputational sanctions are more effective on large organizations and on important organizations that provide network access and transit to many other organizations. This result is consistent with the intuition that the value of reputation and the costs of reputational sanctions are much higher for these organizations because of the large and complex networks at stake and their liabilities to others. W

Limitations

- First, we show that reputational sanctions in the form of an inclusion in the top-10 list is a cost-efficient way to shift a greater share of liability for security vulnerabilities to security-negligent organizations.

- Our reputational sanctions focus on security vulnerabilities prior to data breaches. Resolving such vulnerabilities in time can help prevent further breaches.