

Publicizing a firm's security levels may strengthen security over time, study finds

September 27 2018



Credit: CC0 Public Domain

Cyberattacks grow in prominence each and every day; in fact, 2017 was the [worst year to-date](#) for data breaches, with the number of cyber incidents targeting businesses nearly doubling from 2016 to 2017.

Now, new research from the UBC Sauder School of Business has quantified the [security](#) levels of more than 1,200 Pan-Asian companies in order to determine whether increased awareness of one's security levels leads to improved defense levels against cybercrime.

The study found that when cyberattacks were less likely to directly harm a company, organizations were unlikely to prioritize security improvements. Firms were more likely to fix issues related to spam emails originating from their compromised computers, but failed to act when they were found to host phishing websites on their servers. Most of the firms with phishing websites are actually hosting service providers.

The researchers conducted a randomized field experiment on organizations in Hong Kong, China, Singapore, Macau, Malaysia and Taiwan—which were chosen for their significant economic development as well as rapid adoption of technologies. The experiment evaluated each organization's preparedness against two distinct security issues: spam emissions and phishing website hosting. Spam usually consists of unsolicited bulk messages sent out by compromised "zombie" computers controlled by cyber attackers, while phishing refers to fraudulently obtaining sensitive information, such as passwords and [credit card details](#) for malicious reasons.

"For companies hosting phishing websites, there were fewer incentives to crack down on the sites since they were operated by paying customers and the sites failed to negatively impact the company itself," explains Gene Moo Lee, study co-author and assistant professor of Accounting and Information Systems at the UBC Sauder School of Business.

The researchers developed and assigned an information security score, similar to the idea of Moody's and Standard and Poor's credit ratings, to each organization. The score can be used as an indicator of each organization's security vulnerabilities.

The security results from each company were then [published online](#). According to Lee, publicizing firms' security levels not only leads to greater transparency, but it could also be used to strengthen their security over time. In addition, organizations with poor performance could face greater pressure from their customers and a loss of reputation.

"The ever-increasing number of cyberattacks motivated my co-authors and I to explore a more effective way to enhance the security awareness of organizations and the general public," explains Lee. "By establishing a ranking scheme of firms against online scams, we hope this will heighten firms' awareness to address suboptimal security issues."

For Lee, cybersecurity is an international concern that needs to be managed more effectively. "Many organizations don't understand 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," he said. "Our hope with this research is that companies improve their security levels to prevent the potential of cyberattacks from happening in the first place. And, ultimately, the goal of our research is to provide insights for cybersecurity policy makers."

["Information Disclosure and Security Policy Design: A Large-Scale Randomization Experiment in Pan-Asia"](#) was recently presented at the Workshop on Economics of Information Security. It was co-authored by Yun-Sik Choi and Andrew B. Whinston from the University at Texas in Austin, Shu He from the University of Connecticut, and Yunhui Zhuang and Alvin Chung Man Leung from the City University of Hong Kong.

Provided by University of British Columbia

Citation: Publicizing a firm's security levels may strengthen security over time, study finds

(2018, September 27) retrieved 19 April 2024 from <https://phys.org/news/2018-09-firm.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.