Association for Information Systems

AIS Electronic Library (AISeL)

ICIS 2022 TREOs

TREO Papers

12-12-2022

Are Bug Bounty Programs Equally Beneficial to All Companies? An Empirical Analysis of Cybersecurity and Crowdsourcing

Shuhua Wu
Temple University, shuhua.wu@temple.edu

Aleksi Aaltonen
Temple University, aleksi@temple.edu

Jason B. Thatcher
Temple University, jason.b.thatcher@gmail.com

Follow this and additional works at: https://aisel.aisnet.org/treos_icis2022

Recommended Citation

Wu, Shuhua; Aaltonen, Aleksi; and Thatcher, Jason B., "Are Bug Bounty Programs Equally Beneficial to All Companies? An Empirical Analysis of Cybersecurity and Crowdsourcing" (2022). *ICIS 2022 TREOs*. 83.
https://aisel.aisnet.org/treos_icis2022/83

This material is brought to you by the TREO Papers at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 2022 TREOs by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

TREO
Technology, Research, Education, Opinion

Are Bug Bounty Programs Equally Beneficial to All Companies? An Empirical Analysis of Cybersecurity and Crowdsourcing

Shuhua Wu, shuhua.wu@temple.edu ; Aleksi Aaltonen, aleksi@temple.edu; Jason Bennett Thatcher, jason.thatcher@temple.edu

Companies allocate significant resources to maintain and improve their cybersecurity. Despite deep investments in in-house security experts, technical solutions, and training employees, firms continue to suffer from cybersecurity breaches (Robert 2020). To identify such cybersecurity vulnerabilities, some companies have started to use 'bug bounties'. Bug bounties offer external organizations and experts "recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities" related to securing firm network resources and data (Wikipedia 2022).

To enlist external help for identifying security threats, companies often partner with crowdsourcing cybersecurity platforms such as HackerOne or BugCrowd, who facilitate setting up and managing "bug bounty programs" designed to spot vulnerabilities (Perlroth 2015). The platforms mediate a relationship between the two groups of cybersecurity actors that have traditionally been often at odds with each other. On the one side, firms offer incentives to hackers, their traditional opponents, in the form of payment for identifying security threats. On the other side, hackers register to platforms and submit vulnerability reports in the hope of securing a bounty. According to the HackerOne (2021) report, at least 2000 companies and government agencies use the platform as a means to crowdsource bugs from hackers.

Despite the increasing popularity of bug bounty programs, few papers have evaluated whether bug bounty programs are similarly beneficial to all companies. In practice, small companies tend to have limited resources to hire information security experts compared to their larger counterparts. Yet, they are more frequently under cyber-attack, and 60% of them would go out of business within six months after cyber-attacks (Steinberg 2019). As a result, small companies may rely more heavily on lower-cost bug bounty programs. This leads to our exploratory research questions: Are bug bounty programs equally beneficial to all companies? What factors might moderate the benefit derived from bug bounty programs?

To address these research questions, we will leverage the resource-based view (RBV) and employ a combination of public data from the HackerOne website and a data breach chronology provided by Privacy Rights Clearinghouse to evaluate how bug bounties impact firm security. Our study will offer theoretical and practical insights to researchers and practitioners interested in cybersecurity and crowdsourcing by answering these questions.

References:

The 2021 hacker report. (n.d.). Retrieved September 28, 2022, from https://www.hackerone.com/lp/resources/2021-hacker-report

Perlroth, N. (2015, June 8). HackerOne connects hackers with companies and hopes for a win-win. The New York Times. Retrieved September 29, 2022, from https://www.nytimes.com/2015/06/08/technology/hackerone-connects-hackers-with-companies-and-hopes-for-a-win-win.html

Potter, R. (2020, November 3). Council post: Cfos can prove the value of cybersecurity investments: Here's how. Forbes. Retrieved September 28, 2022, from https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2020/11/04/cfos-can-prove-the-value-of-cybersecurity-investments-heres-how/?sh=10169c8f1927

Steinberg, S. (2020, March 9). Cyberattacks now cost companies $200,000 on average, putting many out of business. CNBC. Retrieved September 29, 2022, from https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

Wikimedia Foundation. (2022, September 26). Bug Bounty program. Wikipedia. Retrieved September 28, 2022, from https://en.wikipedia.org/wiki/Bug_bounty_program

Presentation at TREO Talks in conjunction with the 43rd International Conference on Information Systems, ICIS 2022
TREO Talks are not peer-reviewed and not a formal part of the ICIS 2022 Proceedings
All TREO Talks are available in the TREO Talks section of the AIS e-Library