# Experience and Efficiency in Vulnerability Resolution on Bug Bounty Platforms (Research-in-progress)

**Ali Ahmed**[1]
E. J. Ourso College of Business,
Louisiana State University, USA

**Ho Cheung Brian Lee**
Smeal College of Business,
Pennsylvania State University, USA

**Amit Deokar**
Manning School of Business,
University of Massachusetts Lowell, USA

## Abstract

In cybersecurity, bug bounty programs have emerged as a new method of identifying security vulnerabilities. Despite the growing interest in studying bug bounty programs, it remains unclear how firms collaborate with online hackers on an open bug bounty platform. In this paper, we examine how a firm's experience of working with hackers affects its efficiency in resolving security vulnerabilities on a bug bounty platform. We focus on the collaboration aspect of hackers and firms in an open platform. Using a dataset obtained from a leading bug bounty platform, our initial results suggest an inverted U-shaped relationship between the firm's vulnerability resolution time and the number of vulnerabilities resolved in the past. Interestingly, firms may perform worse (i.e., a long resolution time) as they gain more experience at low to moderate levels of experience. However, once the firms have gained sufficient experience, a positive learning effect kicks in, i.e., vulnerability resolution times decrease with the increase in experience at moderate to high levels of experience. We suggest that firms over-generalize their experience of working with hackers. Resolution experience gained while working with one hacker cannot be sufficiently applied to another hacker.

**Keywords:** Bug bounty, economics of information security, crowdsourcing, organizational learning.

[1] Corresponding author. aliahmed@lsu.edu

## INTRODUCTION

Cybersecurity attacks and data breaches pose a significant and increasing threat to all kinds of organizations. Most of these attacks and breaches are due to the security vulnerabilities present in the information systems of these organizations. Organizations use various techniques and methods to discover hidden vulnerabilities present in their systems. In recent years, crowdsourced penetration testing, also known as crowdsourced vulnerability discovery or *bug bounty*, has become an emerging practice for discovering hidden vulnerabilities. In this method, a crowd of ethical hackers (hereafter referred to as hackers for simplicity) outside the organization is asked to look into an organization's systems to find and report vulnerabilities (Kuehn and Mueller 2018). Hackers are rewarded for responsibly disclosing security vulnerabilities not previously known to the organization. The organizations can design their reward policies and list specific assets for which they are interested in bug bounty. Almost all major technology companies, such as Mozilla, Facebook, Google, Apple, and many other non-tech companies, including the US Department of Defense, have been using bug bounty programs to effectively secure their systems (Kuehn and Mueller 2014). Moreover, in recent years, several bug bounty platforms have emerged, offering firms an affordable and efficient way to launch and manage bug bounty programs (Ahmed et al. 2021). These platforms enable firms to set up reward policies, list assets, process payments, and leverage a large base of hackers for crowdsourced vulnerability discovery (Zhao et al. 2015). Despite many benefits, firms face the key challenge of efficiently resolving or patching[2] the reported vulnerabilities (Al-banna et al. 2018). If vulnerabilities are not actively patched, it introduces inefficiencies into the bug bounty

[2] Traditional literature on vulnerability disclosure and discovery uses "patching" for removing vulnerabilities. However, more recent literature on bug bounty programs and the industry more commonly uses "resolution" for fixing the vulnerabilities. Therefore, *patching* and *resolution* are used interchangeably throughout the paper.

program. Delays in patching not only increase the risk of exploitation but also diminish the potential benefits of running such programs. Therefore, the vulnerability resolution time is a key measure of the efficiency of a bug bounty program.

One key challenge in resolving reported vulnerabilities on bug bounty platforms is managing a large base of hackers. Like many other online communities, online hackers' characteristics on these platforms are dynamic and evolving (Faraj et al. 2011). Inadequately fitting past experiences in working with hackers may harm a firm's vulnerability resolution efficiencies. Hackers on bug bounty platforms vary widely in terms of experience and background, which leads to significant differences in the quality and clarity of the information they provide. Furthermore, the process of extracting more information about a reported vulnerability can also vary from hacker to hacker, potentially reducing resolution efficiencies. Additionally, unlike traditional offline work environments, online platforms lack a shared identity or culture, making it difficult for firms to gauge hackers' commitment, communication style, and reliability (Lykourentzou et al. 2016). As a result, it is uncertain whether firms can effectively learn from past interactions with hackers to improve their vulnerability resolution efficiencies on bug bounty platforms.

Although research has examined the working relationship between teammates and how a professional's collaboration experience may alter their future working performance (Huckman et al. 2009), studies related to how firms collaborate with online communities are scant. Further, the economics of information security literature primarily focused on the incentives and characteristics of the hackers and the patching propensities of vulnerabilities by the organizations in non-bug bounty environments (e.g., Arora et al. 2010; Hata et al. 2017; Kannan and Telang 2005). In this paper, we explore how an organization's experience working with hackers impact

its vulnerability resolution efficiency on an open platform. A key question we seek is whether the experience a firm gains from working with hackers can be leveraged to enhance its ability to resolve more efficiently. If firms learn from this experience, we further ask whether this learning is limited to interactions with familiar hackers or if it can be applied to those who have never previously engaged with the firm. Specifically, we examine the relationship between a firm's vulnerability resolution experience and the vulnerability resolution time on a bug bounty platform. Using a dataset from a leading bug bounty platform, we aim to provide empirical evidence on the relationship between a firm's vulnerability resolution experience and vulnerability resolution time.

## THEORY AND HYPOTHESIS DEVELOPMENT

Theoretical developments in organizational learning (Crossan et al. 1999) and crowdsourcing literature such as Blohm et al. (2018) guide our understanding of how a firm's security team gains knowledge and experience over time as they interact with the hackers on a bug bounty platform. Organizational learning is defined as the change in an organization's performance, such as problem-solving outcomes, production, financial outlook, or task completion times, as the organization acquires experience (Argote et al. 2009; Dutton and Thomas 1984). In the context of bug bounty platforms, as organizations harness the wisdom of the crowd (i.e., hackers), they may learn to work and collaborate with hackers to resolve reported vulnerabilities. This learning may be reflected in a measurable metric, such as the resolution time of these vulnerabilities. We propose that if organizations learn while working with the hackers, their vulnerability resolution efficiencies may change as they gain more experience.

While it is known that experience generally improves firm performance through utilizing the knowledge of involved stakeholders (e.g., Reagans et al. 2005), the dynamic nature of the

online bug bounty communities leads to higher uncertainty in the communication processes and resolution outcomes. The working experience with one or a few hackers may not necessarily apply to the work process with a new reporting hacker. That is, with limited or no experience, performance can suffer due to an "over-generalization" of experience. Researchers have studied the over-generalization of experience by analyzing the relationship between limited experience and spurious successes or failures (Haleblian and Finkelstein 1999; Musaji et al. 2020; Zhao and Olivera 2006). On the one hand, spurious success can reduce the motivation to learn from potential or near-failures. On the other hand, a spurious failure can replace or modify a potentially reliable problem-solving process with an unreliable process. Thus, both spurious successes, as well as spurious failures are detrimental to performance.

We posit a similar phenomenon in the vulnerability resolution process. Firms with limited experience of collaborating with hackers may encounter spurious successes or failures. In contrast, firms with more experience may be able to identify and select reliable problem-solving methods and routines that can be generalized to various situations. Thus, at low levels of experience, we expect to see an increase in resolution time as experience increases due to the over-generalization of limited experience (Haleblian and Finkelstein 1999). The experience gained from working with one hacker may not apply to a report submitted by a different hacker. Therefore, we propose that when firms have a limited amount of working experience, firms inappropriately generalize their experience, which leads to an upward trend in vulnerability resolution time. Thus, at low or moderate levels of experience, a firm would take longer to resolve the reported vulnerabilities as they gain experience. We formally posit hypothesis H1 as:

*H1. At low or moderate levels of experience, a firm's vulnerability resolution time increases as firms gain more vulnerability resolution experience.*

However, once firms have gained high levels of experience working with hackers, the inappropriate generalization or over-generalization effect reduces due to reliable problem-solving processes. Levitt and March (1988) emphasize how organizations' reliable problem-solving routines and processes improve future performance. A routine is a repetitive pattern of interdependent tasks performed by multiple members of an organization (Feldman and Pentland 2003). Routines help organizations perform faster and more reliably (Cohen and Bacdayan 1994). We suggest that firms on bug bounty programs develop reliable routines after gaining sufficient experience working with hackers. Once the firms have gained sufficient working experience with hackers, the learning effect of experience kicks in; this learning effect leads to a downward trend in vulnerability resolution time. We posit hypothesis H2 as:

*H2. At moderate to high levels of experience, a firm's vulnerability resolution time decreases as firms gain more vulnerability resolution experience.*

Furthermore, based on hypotheses H1 and H2, as resolution time first increases and then decreases with the increase in the firm's experience, the relationship between vulnerability resolution experience and vulnerability resolution time will form an inverted U-shaped relationship. Thus, we can also posit that there must be a turning point in the relationship between firm experience and resolution time. Formally, we propose H3 as follows:

*H3. A firm's vulnerability resolution time has an inverted U-shape relationship with the vulnerability resolution experience. Thus, a turning point exists between vulnerability resolution experience and vulnerability resolution time.*

*H4. The turning point of the inverted-U relationship between the firm's experience and vulnerability resolution time decreases (shifts left) as the firm gains more experience working with the same hacker.*

## STUDY CONTEXT AND DATA

To conduct this study, we have gathered a dataset from one of the leading bug bounty platforms. We gathered 176,000 vulnerability reports submitted to over 300 firms running bug bounty programs on the platform. For each vulnerability report, we can identify the firm it was submitted to, the hackers who submitted it, and the timestamp when the report was marked as resolved by the firm. In this data, out of 176,000 reports, approximately 10,000 reports have been publicly disclosed with detailed information on the vulnerability resolution process by the firms. These detailed reports provide information on the date and time of the reporting of the vulnerability, the severity (i.e., none, low, medium, high, critical) of the vulnerability, the bounty amount paid by the firm, all the interactions between the hacker and the firm's security team, and the date and time of the resolution of the vulnerability. Using these disclosed reports, we analyze the firm's resolution time with the change in the firm's experience.

## CONCLUSION AND INITIAL FINDINGS

Using multiple econometric specifications, our initial results suggest that the firms' vulnerability resolution experience doesn't have a non-linear relationship with the firms' resolution time. Firms initially experience longer resolution times as they gain experience working with hackers. However, after reaching a certain level of experience, a positive learning effect occurs, leading to faster resolution times as firms continue to accumulate experience. We also found evidence of over-generalization, meaning that the experience gained from working with one hacker does not easily transfer to others unless the firm has interacted with a large and diverse group of hackers. These findings can have several theoretical and practical implications for vulnerability resolution and bug bounty programs.

## REFERENCES

Ahmed, A., Deokar, A., and Lee, H. C. B. 2021. "Vulnerability Disclosure Mechanisms: A Synthesis and Framework for Market-Based and Non-Market-Based Disclosures," *Decision Support Systems*, Elsevier, pp. 113586–113586.

Al-banna, M., Schlagwein, D., Bertino, E., Barukh, M. C., and Schlagwein, D. 2018. "Friendly Hackers to the Rescue : How Organizations Perceive Crowdsourced Vulnerability Discovery Friendly Hackers to the Rescue : How Organizations Perceive Crowdsourced Vulnerability Discovery," *PACIS 2018 Preceedings*.

Argote, L., Beckman, S. L., and Epple, D. 2009. "The Persistence and Transfer of Learning in Industrial Settings," in *The Strategic Management of Intellectual Capital*. (https://doi.org/10.1287/mnsc.36.2.140).

Arora, A., Krishnan, R., Telang, R., and Yang, Y. 2010. "An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure," *Information Systems Research* (21:1), pp. 115–132. (https://doi.org/10.1287/isre.1080.0226).

Blohm, I., Zogaj, S., Bretschneider, U., and Leimeister, J. M. 2018. "How to Manage Crowdsourcing Platforms Effectively?," *California Management Review* (60:2), pp. 122–149. (https://doi.org/10.1177/0008125617738255).

Cohen, M. D., and Bacdayan, P. 1994. "Organizational Routines Are Stored as Procedural Memory: Evidence from a Laboratory Study," *Organization Science* (5:4), pp. 554–568. (https://doi.org/10.1287/orsc.5.4.554).

Crossan, M. M., Lane, H. W., and White, R. E. 1999. "An Organizational Learning Framework: From Intuition to Institution," *Academy of Management Review* (24:3), pp. 522–537. (https://doi.org/10.5465/AMR.1999.2202135).

Dutton, J. M., and Thomas, A. 1984. "Treating Progress Functions as a Managerial Opportunity.," *Academy of Management Review* (9:2), pp. 235–247. (https://doi.org/10.5465/amr.1984.4277639).

Faraj, S., Jarvenpaa, S. L., and Majchrzak, A. 2011. "Knowledge Collaboration in Online Communities," *Organization Science* (22:5), INFORMS, pp. 1224–1239.

Feldman, M. S., and Pentland, B. T. 2003. "Reconceptualizing Organizational Routines as a Source of Flexibility and Change," *Administrative Science Quarterly* (48:1), pp. 94–118. (https://doi.org/10.2307/3556620).

Haleblian, J., and Finkelstein, S. 1999. "The Influence of Organizational Acquisition Experience on Acquisition Performance: A Behavioral Learning Perspective," *Administrative Science Quarterly*. (https://doi.org/10.2307/2667030).

Hata, H., Guo, M., and Babar, M. A. 2017. "Understanding the Heterogeneity of Contributors in Bug Bounty Programs," *International Symposium on Empirical Software Engineering and Measurement* (2017-Novem), pp. 223–228. (https://doi.org/10.1109/ESEM.2017.34).

Huckman, R. S., Staats, B. R., and Upton, D. M. 2009. "Team Familiarity, Role Experience, and Performance: Evidence from Indian Software Services," *Management Science* (55:1), pp. 85–100. (https://doi.org/10.1287/mnsc.1080.0921).

Kannan, K., and Telang, R. 2005. "Market for Software Vulnerabilities? Think Again," *Management Science* (51:5), pp. 726–740. (https://doi.org/10.1287/mnsc.1040.0357).

Kuehn, A., and Mueller, M. 2018. "Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities," *SSRN Electronic Journal*, pp. 1–16. (https://doi.org/10.2139/ssrn.2418812).

Levitt, B., and March, J. G. 1988. "Organizational Learning," *Annual Review of Sociology* (14:1), Annual Reviews 4139 El Camino Way, PO Box 10139, Palo Alto, CA 94303-0139, USA, pp. 319–338.

Lykourentzou, I., Wang, S., Kraut, R. E., and Dow, S. P. 2016. *Team Dating: A Self-Organized Team Formation Strategy for Collaborative Crowdsourcing*, presented at the Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp. 1243–1249.

Musaji, S., Schulze, W. S., and De Castro, J. O. 2020. "How Long Does It Take to Get to the Learning Curve?," *Academy of Management Journal* (63:1), pp. 205–223. (https://doi.org/10.5465/amj.2017.1145).

Reagans, R., Argote, L., and Brooks, D. 2005. "Individual Experience and Experience Working Together: Predicting Learning Rates from Knowing Who Knows What and Knowing How to Work Together," *Management Science* (51:6), INFORMS, pp. 869–881.

Zhao, B., and Olivera, F. 2006. "Error Reporting in Organizations," *Academy of Management Review*. (https://doi.org/10.5465/AMR.2006.22528167).

Zhao, M., Grossklags, J., and Liu, P. 2015. "An Empirical Study of Web Vulnerability Discovery Ecosystems," *Proceedings of the ACM Conference on Computer and Communications Security* (2015-Octob), pp. 1105–1117. (https://doi.org/10.1145/2810103.2813704).