By Nidhi Hegde

Bug Bounty and Incident Response

T. Walshe and A. Simpson, "**An Empirical Study of Bug Bounty Programs**," 2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF), London, ON, Canada, 2020, pp. 35-44, doi: 10.1109/IBF50092.2020.9034828.

Bug bounty programs, which offer rewards to security researchers or “ethical hackers” to find and disclose vulnerabilities in software, are becoming increasingly popular. This approach has been adopted in various areas, such as e-voting systems, government systems, and self-driving cars. The paper does an empirical study on the use of rewards programs and provides an economic analysis to explain why some companies are increasingly utilizing the global network of security expertise offered by hackers instead of hiring additional staff. The cost of employment of a software engineer is one criterion that can be used to evaluate the cost-effectiveness of hiring staff versus offering rewards to ethical hackers. Bug bounty programs are being integrated into secure software development lifecycle (SDLC) frameworks to aid security teams in the release and maintenance phases. Many large organizations, such as Google, Facebook, and Microsoft, host their own bug bounty and vulnerability rewards programs, while many smaller organizations use bug bounty platforms such as HackerOne, BugCrowd, and Cobalt to advertise their programs. This crowdsourced approach to security brings together hackers from many backgrounds and disciplines, resulting in a wide range of approaches to finding vulnerabilities that might not otherwise be achieved by an organization's security team.

The analysis of the results of the bug bounty programs indicates that the cost of running such programs is highly dependent on the success of hackers in finding vulnerabilities, as well as the rewards structure in place. The average annual cost of operating a full-time program is greater than the cost of hiring an additional software engineer. The severity of vulnerabilities cannot be predicted before the program is launched, so the rewards structure can be altered if a large number of high-severity vulnerabilities are reported. There is a weak correlation between the success of a program and the average bounty payout, as hackers value the challenge or opportunity to learn almost as much as the bounty payouts when selecting programs in which to participate. The authors also mention that the participation of hackers on BugCrowd and HackerOne is very skewed, with the top 100 users contributing a significant proportion of overall reports. Small and medium businesses make up 50% of businesses using bug bounty platforms, indicating that operating a bug bounty program may be viable for a business regardless of size.

By Nidhi Hegde

Akgul, Omer & Eghtesad, Taha & Elazari, Amit & Gnawali, Omprakash & Grossklags, Jens & Mazurek, Michelle & Votipka, Daniel & Laszka, Aron. (2023). **Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem**. 10.48550/arXiv.2301.04781.

The paper discusses how bug-bounty programs are incentives for independent security experts to find vulnerabilities in a company's products and report them in exchange for rewards. The authors say that these programs suffer from inefficiencies, such as receiving invalid or duplicate reports, competing to attract productive hunters, and hunters facing uncertainties regarding their findings and rewards. They also suggest that addressing these issues could improve the security posture of many companies and improve software security more broadly.

To address these gaps, the authors conducted three studies to answer two research questions: What are the factors that hunters consider and challenges they face when participating in bug bounties? How important are these factors to hunters, and why? The authors found that the most salient benefits of bug bounties are monetary, and they suggest that stakeholders prioritize factors that hunters consider to be most important.

Based on their study the authors recommend bug-bounty programs can increase scope and rewards, but both require additional resources. They emphasize on communication being a significant challenge, and increasing staffing is the most effective solution to address responsiveness. They also suggest that providing frequent and transparent updates can reduce uncertainty and improving overall communication can reduce unexpected responses. Bug-bounty programs should make scopes and bounty tables clear and provide examples with payouts per bug.

They also provide certain points that can be improved by the bug-bounty platforms. Bug-bounty platforms can improve their support and mediation for hunters, increase transparency and communication, provide more guidance and training, and reduce uncertainty through insurance policies or managing the triaging process. They can also focus on improving learning resources and integrating them with previously disclosed bugs. Additionally, bug-bounty platforms can provide a wide range of payment mechanisms, standardize interfaces between programs, and promote well-maintained or societally important programs to distribute hunters' attention.

Kiran Sridhar, Ming Ng, "**Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties,**" Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyab007, https://doi.org/10.1093/cybsec/tyab007

As discussed in previous items as well, bug bounty programs are becoming increasingly popular among companies. We also know that there has been limited empirical research in this area, and researchers have yet to determine the effects that a company's revenue, industry, and brand profile have on the number of reports their programs receive. This paper conducts a study which examines HackerOne's database from August 2014 to January 2020, finds that smaller companies, regardless of their brand profile, can derive value from bug bounties, while programs receive fewer reports as they grow older.

The study finds that the supply of hackers is price inelastic and that non-monetary factors such as experience and reputation play a significant role in motivating them. The paper also points out that brand profile and revenue have an insignificant impact on the reports companies receive. In terms of industry effects, companies in the finance and retail industries receive fewer valid reports than companies in other industries, and that medical companies receive fewer reports as well. The number of new programs has a statistically insignificant effect on the reports companies receive. The authors conclude by suggesting that the study's findings are positive for small and medium-sized enterprises that lack the resources to offer generous bounties, and that bug bounty programs democratize access to IT talent.

Aaltonen, Aleksi, and Yiwen Gao. "**Does the Outsider Help? The Impact of Bug Bounty Programs on Data Breaches.**" (August 20, 2021). Fox School of Business Research Paper (2021).

This paper discusses the pros and cons of bug bounty programs, which allow outsiders to report vulnerabilities in a company's systems. While such programs can decrease the risk of data breaches over time by finding and fixing vulnerabilities, they also attract black hat hackers who may attack the website with malicious intentions, publish the vulnerability online, or sell it on the market. Moreover, bug bounty programs can be expensive and may divert resources from other security strategies. The article suggests that the impact of bug bounty programs on data breaches is an empirical question and highly risk-averse firms may benefit from such programs. Unlike the items discussed above, this paper challenges the assumption that crowdsourcing is always beneficial for firms and contributes to both cybersecurity and crowdsourcing literature.

By Nidhi Hegde

Van der Kleij R, Kleinhuis G, Young H. **Computer Security Incident Response Team Effectiveness: A Needs Assessment.** Front Psychol. 2017 Dec 12;8:2179. doi: 10.3389/fpsyg.2017.02179. PMID: 29312051; PMCID: PMC5733042.

Cyber threats, such as state actors and occupational criminals, pose significant economic and national security challenges that need to be addressed. It is essential to protect the critical infrastructure and respond to incidents quickly and effectively. We know that Computer Security Incident Response Teams (CSIRTs) play a vital role in incident response and achieving benefits such as systematic incident handling, minimizing the consequences of incidents, and learning from incidents. The author mentions that CSIRTs often have to work on an ad hoc basis, in close cooperation with other teams, and in time constrained environments. Hence under these working conditions CSIRTs would be likely to encounter problems. This paper discusses the variability in issues that Computer Security Incident CSIRTs face and the need for customized solutions for improving their performance. The study identifies common needs for improving CSIRT performance, including better organizational-level learning from incidents, training in both technological and soft skills, developing multiteam systems for incident handling, improving incident assessment processes through collaborative sensemaking, redesigning work processes, and providing better tools for team collaboration. The authors emphasize that solutions for one CSIRT may not work for others due to differences in factors such as type of CSIRT, type of organization, size, and services offered. The success of a CSIRT depends on technical resources, knowledge, skills, and teamwork within and outside the organization. To reach their full potential, CSIRTs must establish means of communication, build relationships, and share threat, attack, and vulnerability information with each other. However, the creation of a CSIRT does not ensure success, and many fail due to their ad hoc working conditions and crisis situations.

By Nidhi Hegde

M. Ioannou, E. Stavrou and M. Bada, "**Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination**," 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 2019, pp. 1-4, doi: 10.1109/CyberSecPODS.2019.8885240.

The number of cyber-attacks has been rising in recent years, with incidents such as the Equifax breach and the release of NSA exploits leading to a proliferation of ransomware attacks. The financial costs of security breaches include both direct and indirect costs, and organizations should have effective incident management processes to minimize their impact. A Computer Security Incident Response Team (CSIRT) typically manages and coordinates incident management processes within an organization. However, the weakest link in the chain remains human error, so organizations should invest in developing a cybersecurity culture to minimize this risk. This paper conducts detailed research to identify issues that limit communication and cooperation within a CSIRT and provides approaches that can help address these issues.

The paper discusses following factors affecting the development of a cybersecurity culture in detail:

1. Clarity of Policies
2. Assumptions Made by Management Members
3. Points of Focus for Policy Makers
4. Communication Development Efforts
5. Cooperation Development Efforts
6. Csirt's Effectiveness Improvement

The study identifies several challenges that affect communication, coordination, and cooperation within a CSIRT, which can hinder the establishment of a cybersecurity culture. These include lack of teamwork spirit and trust, lack of confidence, fear of personal exposure, new teams not including existing staff, lack of collaborative behavior training, and lack of KPIs (Key Performance Indicators) related to communication and coordination. In order to address these challenges, the authors recommend following measures:

1. Investing in creating a culture of collaboration.
2. Providing accreditation and training to staff, including existing staff in new teams.
3. Providing technical and collaborative behavior training and establishing KPIs related to internal communication and coordination.
4. Conducting frequent audits to identify weaknesses and take corrective actions.

By Nidhi Hegde

Zoom Recording Details

One of the team members, Sumedh talked on following 2 items which were similar to the readings that I did. Below are some interesting points from the discussion:

1. S. S. Malladi and H. C. Subramanian, "Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations," in IEEE Software, vol. 37, no. 1, pp. 31-39, Jan.-Feb. 2020, doi: 10.1109/MS.2018.2880508.
   Here he talked about best practices recommended by the authors in following five main Bug Bounty Program areas: scoping of BBPs, timing of crowd engagement, submission quality, firm-researcher communication, and hacker motivation.

2. Aaron Yi Ding, Gianluca Limon De Jesus, and Marijn Janssen. 2019. Ethical hacking for boosting IoT vulnerability management: a first look into bug bounty programs and responsible disclosure. In Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing (ICTRS '19). Association for Computing Machinery, New York, NY, USA, 49–55. https://doi.org/10.1145/3357767.3357774

   Here talked about potential of using Bug Bounty Programs to enhance IoT vulnerability management. The paper aims to develop practical guidelines for companies, consumers, and regulators to demystify the complex issue of IoT security and shed light on how such programs can be integrated with existing security practices to further boost overall IoT security.

   Recording Link:
   https://purdue0-my.sharepoint.com/:v:/r/personal/lee4468_purdue_edu/Documents/CS523/ResearchAssignment6.mp4?csf=1&web=1&e=cGcShP