Bloomberg BNA

Privacy and Security Law Report®

Data Security

In an age of ceaseless cyberattacks and high stakes data breaches, vulnerability reward programs—also known as Bug Bounty programs—to reward external ''security researchers'' for discovering and reporting an organization's data security flaws are an increasingly popular security initiative, the authors write, setting out the basic ingredients for establishing such a program.

Bug Bounty Programs: Is a Vulnerability Incentives Program Right for You?

BY BRIAN HENGESBAUGH AND HARRY A. VALETK

The public and private affairs of humans today depend entirely on secure and stable interconnected networks. No business, government or institution can function effectively without them. Achieving perfect security and stability in every internal and external system, however, is impossible. And finding and retaining professional talent with the right mix of technical skills and organization experiences to build and maintain optimum security is nearly impossible. So how can organizations achieve more secure computing environments, identify vulnerabilities early and efficiently, and still execute in a way that mitigates the potentially adverse impact to their brands?

Enter the *Bug Bounty* programs. In an age of ceaseless cyberattacks and high stakes data breaches, these increasingly popular security initiatives serve the private sector as a public resource.

Vulnerability Reward Programs

Bug Bounty programs—also known as vulnerability reward programs (VRPs)—are publicly-posted reward programs, instituted by organizations seeking to formalize relationships with external ''security researchers.'' The goal is to spot technical vulnerabilities in code or systems early, and encourage the security research community to help patch code vulnerabilities or create system mitigations. *Bug Bounty* programs unveil alarming revelations that eventually end up preventing widespread damage to customers and companies alike. Security researchers, ethical hackers and other enthusiasts from all over the world often participate.

Companies currently using *Bug Bounty* programs report considerable success paying ''security researchers'' monetary or other incentives (e.g., travel miles) for vulnerability information on software, code or products

 ISSN 1538-3423

before or shortly after they go to market. Global companies across many industry sectors have been using *Bug Bounty* programs effectively for certain publicly-facing systems. And intermediary companies like Bugcrowd and Hackerone now exist to just help companies interface with the security researcher community, managing over 160 *Bug Bounty* corporate programs.

Some companies consider it a significant risk to formally invite hacking or any form of sanctioned attack on their networks that could result in unforeseen problems or system instabilities.

Other companies, however, consider it a significant risk to formally invite hacking or any form of sanctioned attack on their networks that could result in unforeseen problems or system instabilities. Those that have this concern also cite to the legal risks that publicly posted *Bug Bounty* programs pose to waiving the rights and remedies afforded under federal law against malicious hackers for damage to corporate networks. To elaborate, the Computer Fraud and Abuse Act (CFAA) criminalizes any intentional access to a computer without authorization, or one which exceeds authorized access, that results in obtaining information from, among other sources, ''any protected computer.'' The term, ''any protected computer,'' is broadly defined to include a computer ''which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.'' And the term ''exceeds authorized access'' means to access a computer with authorization, and then use that access to obtain or alter information in the computer that the person accessing the system is not entitled to obtain or alter.

If a company, therefore, openly invites ''security researchers'' to uncover technological vulnerabilities without limitations, it may inadvertently limit its own ability to subsequently raise a CFAA claim that a hacker accessed that company's protected devices ''without or exceeding authorization.''

Even so, the goal with any *Bug Bounty* program is not perfection or other unachievable goal. It's about intervening and reducing the damage that lapses in security can cause. It's a way of collaborating with a talented community, and turning critics into partners recruited to solve potential security concerns. Built correctly, these *Bug Bounty* programs can also contribute to an enterprise's software development lifecycle, and reduce the number of bugs that leak into production.

Basic Ingredients

So how should you build out your *Bug Bounty* program? What basic ingredients and legal issues should you take into account? Of course, no one-size-fits-all approach exists, and every company must look at this within the context of their industry, internal culture, regulatory framework and overall operational risks. Despite those foreseeable variations, a few important business and legal elements should be part of every *Bug Bounty* program.

1. Comply with applicable law. No matter what, every *Bug Bounty* program must comply with applicable law, including tax reporting obligations. To that end, your *Bug Bounty* terms must prohibit rewards or payments to individuals listed on the Federal Bureau of Investigation's Cyber's Most Wanted, a sanctions list (in the U.S. or elsewhere) or anyone situated in a country on a sanctions list (e.g., Iran, Lybia, North Korea, Syria, Sudan).

2. Establish program rules. Whenever you're dealing with a community of external stakeholders, clarity pays. Among other points, establish and publish your program rules that specify the types of vulnerabilities you consider in-scope for an award, and the range of compensation based on risk and severity to your organization. Some companies cap awards, others don't. Specifically exclude the authors of the vulnerability code, as well as any illegal activity or certain types of disruptive detection methods like denial-of-service or brute force attacks. For those ''security researchers'' uninterested in monetary rewards, offer to provide attribution for marketplace credibility or donate eligible funds to an established and company-approved charity. Limit rewards only to individuals.

3. Require pre-registration. An increasing number of companies are requiring ''security researchers'' to pre-register or provide verifiable identification when making a bounty claim. This helps avoid payments to the very authors of those vulnerabilities codes, and better ensures compliance with trade sanctions and other legal compliance or industry requirements, policies and procedures.

4. Exclude third party sites and systems. Restrict trespassing or the use of any research performed on websites, software, or networks hosted or operated by third parties to exploit security vulnerabilities in your environment. The last thing your *Bug Bounty* program should do is incentivize potential attacks or disruptions on the technical environments of others. This includes websites or systems operated by corporate clients, business partners or service providers. Any testing activities undertaken to uncover a vulnerability must never put individuals at risk, violate applicable law, or in any way disable third party systems.

5. Confidentiality. To be eligible for an award, require that identified vulnerabilities be first brought to your attention, and, thereafter, subject to a gag period (e.g., 90 days) or non-disclosure agreement to keep vulnerability details confidential indefinitely. Doing so provides the company with a way to repair a vulnerability and deploy a solution on its own terms, thereby effectively managing the potential security risks to its environment.

6. Incentivize the right outcomes. Write your rules in a way that will incentivize the right outcomes. Limit the program to the identification of technical vulnerabilities. Never reward attempts to penetrate your physical security, access or acquire personal information, or carry out social engineering campaigns against your employees or third party consultants.

7. Exclude availability of rewards for recently acquired operations. Provide a reasonable grace period (e.g., 6 months) before offering rewards for identification of vulnerabilities in newly-acquired companies or

  PVLR ISSN 1538-3423

assets. This will provide internal security professionals with the opportunity to review and update security features in accordance with enterprise standards.

8. Align program with internal stakeholders. Confirm that the program, as envisioned, is fully endorsed and accepted by internal information security, information technology and legal teams before launch. All stakeholders will need to be aligned to ensure proper configuration of the program, and to secure buy-in to the changes in interfacing with the security research community.

9. Establish clear line of communication with the right stakeholders internally. This will depend, in part, on the method you use to facilitate interacting with the security research community. At first, companies relied on e-mails to designated security reporting mailboxes. More recently, however, companies rely on dedicated links where links, videos, and other Proof of Concept and supporting documentation can be uploaded securely. Regardless of what method you use, make sure that your security vulnerability receptacle is staffed appropriately by security professionals qualified to recognize technical vulnerabilities swiftly, and are empowered to escalate issues internally to the right levels within the organization.

10. Retain absolute discretion. Establish rules that provide the company with absolute discretion in determining whether to allow participation by any particular individual, whether to make an award in any case, and if so, in what amount. Various unforeseen factors may come into play in a specific situation, and may influence whether or how much reward is reasonably due. Decide whether or not you wish to waive any claims under CFAA for those who comply with the *Bug Bounty* program's terms.

Conclusion

While it may be safe to say that *Bug Bounty* programs are gaining steam, it's also safe to say that they are **not** without risk. Remember, you're inviting gifted hackers to find flaws in the security of your product, service, or networked environment. That means that you better have a solid internal security team capable of anticipating what those flaws will be and remediating them before any product or service becomes available to the public, since the last thing you want is a marketplace reputation for weak and flawed systems.

Still, with more leading companies agreeing to formally collaborate with the ''security research community'' to uncover their unknowns, and promoting overall awareness, *Bug Bounty* programs are a security risk management option worthy of internal deliberation.

Brian Hengesbaugh is a Principal in the Chicago office of Baker & McKenzie and Chair of the Firm's Global IT/C Data Security Steering Committee. He focuses on global data privacy and data security issues in business transformations, compliance activities, and incident response/ regulatory inquiries. Brian can be reached at brian.hengesbaugh@bakermckenzie.com.

Harry A. Valetk is Of Counsel in the New York office of Baker & McKenzie. He advises multinational clients on global data privacy compliance and cyber security risks. Harry can be reached at harry.valetk@bakermckenzie.com.