Don't Let the Bug Bounties Bite

BY JULIE ENGBLOOM AND PETER FISK

Bug bounty programs have been crawling out of the woodwork as part of comprehensive cybersecurity protocols. The "bug" here refers to unknown security vulnerabilities, and a bug bounty program is a system of paying rewards and giving recognition to outside security researchers who report bugs to the program developer instead of exploiting them. That way, the vulnerability can be fixed ("patched"). These programs have been around since Netscape, which launched its bug bounty program in 1995. Even the Department of Defense runs a program. United Airlines pays in miles. And while many bounty programs start with rewards of $50 or less, Intel and Microsoft currently offer rewards as high as $250,000, through the end of 2018, for reporting certain serious vulnerabilities.

If you are considering a bug bounty program, here are a few key legal issues to address in a written bug bounty policy.

Consider a No-Reward Program at the Start. You might not know how many people will come searching for and finding bugs on your system. For that reason, many companies experiment first with an unpaid reporting program, often called a vulnerability disclosure program. Even if it never evolves into a paid bounty program, it is prudent to have a contact point online for reporting security problems.

Make the Authorization Clear. Bug hunters crawling around a company's electronic systems looking for vulnerabilities are at legal, even criminal, risk. For that reason, it is vital to give authorization in exchange for following your policy.

At the same time, it is vital to set limits. If you only want researchers looking at certain services, apps or web domains, make that clear. Prohibit conduct that harms customers, users and other third parties. Make it clear that you will not be liable for or indemnify researchers for any harm they cause.

Figure Out Your Reward System. Your organization will need to decide how it sets bounties. Policies should be clear about what bugs are eligible for a reward, the range of rewards, and what makes a sufficient report. Make it clear that you retain discretion in setting rewards.

Eligibility for Payment. Most likely, you will need some personal information in order to pay a reward. Make that clear, and also that the researcher is responsible for any taxes that apply. The policy should provide carve-outs for countries or individuals who are ineligible for payment. Many programs also include an alternative to direct payment, which is to donate the reward to a pre-approved charity.

Avoid Disputes. A bug bounty policy should set out the governing law, jurisdiction and dispute resolution forum. Also, be aware that higher rewards are more likely to create litigation risk.

Preserve Your Ability to End the Program. Set out at the start how you can end or modify the bounty program. Many bug bounty programs have time limits. You can also set out how notice will be given if the program is suspended, and when such changes become effective.

Manage Disclosure and Intellectual Property Concerns. One major reason to have a bug bounty program is that it staves off unplanned public disclosure of your vulnerabilities and technology. Make confidentiality a clear part of your policy.

At the same time, many researchers care about getting recognition. Consider whether to give recognition online, or to allow the researcher to announce their results after you have patched a bug. If so, set up a process for doing so.

Last, you will want to retain your right to control disclosure of trade secrets and other confidential information. You may also want to make clear that the bug hunter does not obtain any intellectual property in the process of reporting bugs to you.

Consider Your Commitment. There are a number of vendors who can set up and run a bug bounty program on your behalf. You benefit from their know-how, and it relieves you from hosting the program on your own website. Other organizations run bounty programs entirely on their own.

The important thing is to make sure you devote enough resources to reviewing and responding to reports. And you will want to consult with your counsel on drafting your bug bounty policy. ■

Julie Engbloom is Co-Chair of Lane Powell's Privacy and Data Security Team and assists companies in developing incident response plans and strategies, responding to regulatory actions and defending against data security-related litigation. Reach her at engbloomj@lanepowell.com or 503.778.2183.

Peter C. Fisk is a Commercial Litigation Associate at Lane Powell, practicing in privacy and data security, e-discovery strategy, internal investigations, class actions and other complex cases. Reach him at fiskp@lanepowell.com or 503.778.2180.