Considering a Vulnerability Disclosure Program? Recent Push Raises Questions for General Counsel

This article was published by CircleID on February 10, 2017.

Several years ago, vulnerability disclosure programs, also called "bug bounty" programs, were novel and eyed with suspicion. Given sensitivities and potential liabilities, companies are wary of public disclosure and hackers seeking to exploit research. When a hacker presented a flaw to a company, the company was more likely to be concerned about taking legal action than making a public announcement or offering a reward. That is changing. Vulnerability disclosure programs can improve product and service security, but they present legal and practical challenges that advocates overlook and prudent companies should consider.

Vulnerability Programs Take Shape and Start to Go Mainstream, with Government Prompting

Starting in 2013, many technology companies, like Microsoft, Google, and FitBit,[i] began to implement and expand vulnerability disclosure programs. These programs seek to channel the energy of the hacking and research community, while limiting damage from premature or imprudent disclosures. In recent years, companies outside of the technology sector, like General Motors[ii] and United Airlines,[iii] have implemented varied vulnerability disclosure programs. Startups, like HackerOne, now offer to "surface" your company's vulnerabilities by working with "the global research community."

In 2016, vulnerability disclosure programs became more accepted, with the relatively stodgy Department of Defense offering a bug bounty. In January 2017, the Army released the results of this effort. The report is eye-catching. In a three week period, over 300 hundred people registered to participate. They reported 118 unique and actionable vulnerabilities, resulting in payouts of about $100,000. The first bug was reported within five minutes, and one researcher was able to string together a series of vulnerabilities to move from the public-facing www.goarmy.com to "an internal DoD network" that should have prompted him for credentials. By all accounts, the program was a success.

Looking to expand the use of bug bounty programs, the National Telecommunications and Information Association (NTIA), a government agency that looks at the digital economy, got involved. It convened a multi-stakeholder process to look at public disclosure and various private efforts to manage vulnerabilities. This comes amidst interest in security updates and patching for connected devices, which the security community and government are looking at.

Authors

Megan L. Brown
Partner
mbrown@wileyrein.com

Matthew J. Gardner
Of Counsel
mgardner@wileyrein.com

Practice Areas

Telecom, Media& Technology

Privacy & Cybersecurity

In January 2017, NTIA published preliminary guidance on vulnerability disclosure programs, including a template[iv], Coordinated Vulnerability Disclosures, that provides an overview of basic considerations in creating a vulnerability program and a sample vulnerability disclosure policy. Overall, that guidance broadly promotes disclosure programs.

The NTIA effort, however, seems to gloss over potential dangers in adopting a vulnerability disclosure program. Before your company's Chief Security Officer or IT security team starts developing a vulnerability disclosure program, here are some things to consider.

Benefits of a Vulnerability Program

The appeal of these programs is easy to see. They provide an opportunity for companies to improve cybersecurity by tapping into the collective skills and expertise of ethical hackers and security researchers — skills that may be difficult or impossible to replicate in-house.

Ethical security researchers operate in a grey area. According to a survey conducted by NTIA, Vulnerability Disclosure Attitudes and Actions: A Research Report, 60% of researcher respondents claimed to fear "they may be subject to legal proceedings if they disclose their work." This fear is not unfounded. Researchers and other so-called white hat hackers run the risk of violating various laws, most notably the Computer Fraud and Abuse Act ("CFAA"), which creates civil and criminal penalties for unauthorized access to any protected computer.

Vulnerability disclosure programs seek to clarify the rules of engagement by providing limited authorization for "good faith" testing of a company's information system or products. Depending on the nature of the program and the authorization given, they can allow the public to engage in limited hacking against a company. As long as researchers stay within the bounds of a program's grant of consent, researchers can in theory feel confident that their actions do not violate the CFAA, thereby encouraging reporting. Companies, in turn, may benefit by learning about previously unknown cybersecurity flaws in a controlled manner.

There are Reasons for Caution

Properly managing vulnerabilities presents challenges. Public disclosure — particularly premature disclosure — can scare consumers, inform competitors of weakness, inspire government oversight, result in litigation, and of course, facilitate attacks by hackers exploiting the vulnerability.

The research community is diverse and has varied motives, with some pushing the bounds of ethical and legal behavior. For example, a cybersecurity researcher and hedge fund joined forces to exploit a claimed vulnerability in a medical device to short its manufacturer's stock.[v] Annual security conferences are prime time to promote claimed vulnerabilities, some of which are real and others not.

No company relishes being the public focus of the hacking community. For example, in 2015, two security researchers claimed in Wired magazine that some of Chrysler's vehicles had vulnerabilities. The security researchers worked with Chrysler before disclosing the vulnerability, and Chrysler patched it and issued a recall on the cars.

While Chrysler may have benefitted from learning about the flaw, the disclosure still had ramifications: Chrysler is involved in class action litigation and an investigation by the National Highway Traffic Safety Administration. Class action plaintiffs in court claim that the vulnerability could have turned "vehicles into rolling deathtraps [and could] allow hackers to take remote control of the vehicle's functions, including the vehicle's steering and brakes, to comical or disastrous effect."[vi] Importantly, the litigation and investigation were triggered merely by disclosing the vulnerability — not an actual cyber incident involving a hacked car. The fear of such litigation could be a serious deterrent to active participation in vulnerability disclosure efforts.

Setting up a Vulnerability Disclosure Program

Many IT professionals are interested in these programs. We have identified some of the many issues that companies should consider as they evaluate whether to create or modify a vulnerability disclosure program. Corporate legal departments may want to be involved in considering whether and how to proceed.

- *First, companies must decide whether to adopt a program.* NTIA's sample policy limits a company's right to protect its network from hackers and is maybe overly broad for most companies that want to operate a bug bounty program. The NTIA sample policy would allow would-be hackers to engage in "reverse engineering or circumventing protective measures," and provides broad immunity to any hacker who "submit[s] vulnerability reports through our Vulnerability Reporting Form." Reverse engineering and circumventing protective measures are intrusive, and many companies may not want to authorize activity beyond the permissions afforded under recent interpretations of copyright law and anti-circumvention policies.

- *Second, companies must determine how to scope a program appropriately.* Companies can ease into a program by applying it only to some products, or by limiting it to some service. They can include or exclude their own websites, portals or applications. There are myriad other scoping questions, which really boil down to legal questions, including whether to waive the right to sue for intrusions or hacking, and what restrictions to impose on researchers to benefit from the company's waiver.

- *Third, companies need to evaluate whether they have the resources to properly staff a program.* Quickly evaluating and fixing vulnerabilities is not easy. Many bug bounty programs provide commitments to make public updates on fixes and to publically recognize researchers who identify bugs. Those commitments may not be feasible, especially for companies releasing new products in a competitive market.

- *Fourth, a company should consider how it will resolve reports and whether it will document that resolution, with an eye toward litigation or oversight.* A vulnerability disclosure program will invite negative reports. The company will have to be ready to handle such information, both logistically and substantively. For example, if a company receives a report and does not find it credible or high risk, and decides not to remediate, subsequent government inquiries or litigation might seek internal deliberations about the report.

- *Lastly, a company needs to understand obligations it might have to notify business partners, regulators, and the public.* Receipt of information about alleged vulnerabilities could trigger notification obligations to consumers, government customers, regulators, regulators, or in SEC filings. How will a company handle vulnerabilities that relate to products manufactured or designed by others? If a vulnerability affects a commonly available or commercially sourced network component, will the company notify the vendor?

These are just a few of the issues a company will confront. While the opportunity to improve cybersecurity is promising, in offering a program, a company is effectively consenting to being hacked. If a company decides to adopt a program, it needs to know what options are available and craft a program that is tailored to its particular situation.[vii]

[i] For examples, go to: https://technet.microsoft.com/en-us/security/dn425055.aspx; https://www.google.com/about/appsecurity/programs-home/ (explaining various rewards); https://bugcrowd.com/fitbit

[ii] *See* https://hackerone.com/gm

[iii] *See* https://www.united.com/web/en-US/content/Contact/bugbounty.aspx

[iv] Available at: (https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf)

[v] *See* M. Goldstein, Hedge Fund and Cybersecurity Firm Team Up to Short-Sell Device Maker, N.Y. Times (Sept. 8, 2016)

[vi] *See* Flynn v. FCA US LLC, 2016 WL 5341749 (S.D.Ill. 2016) (granting in part and denying in part defendants' motions to dismiss).