The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 7 April 5, 2017

TECH MEETS LEGAL SPOTLIGHT

Proactive Steps to Prevent Legal Pitfalls in Bug Bounty Programs

By Amy Terry Sheehan

Bug bounty programs that use crowdsourcing methods can help companies identify vulnerabilities that their internal teams may not catch. These programs, however, can also open companies up to a range of legal and business risks, such as publicly exposing user problems caused by the bug researchers, and other flaws, before they are fixed. Michael Yaeger, special counsel in the Litigation Group at Schulte Roth & Zabel, spoke to The Cybersecurity Law Report about how companies can develop programs to minimize those risks, including setting clear terms covering issues such as confidentiality, payments, unauthorized actions and scope. We provide specific examples of program terms to illustrate Yaeger's advice.

See also "*How to Establish and Manage a Successful Bug Bounty Program*" (Mar. 22, 2017).

CSLR: What are some of the advantages of using a bug bounty program to try to discover vulnerabilities?

Yaeger: The benefits are ones you typically would get from crowdsourcing and harnessing the power of markets, which are good at moving information. You may not know exactly who will be the best researcher for this and a bug bounty program lowers your cost of having to locate that person. The benefit is economic.

CSLR: What are some of the legal and business risks?

Yaeger: Companies need to be prepared to patch flaws that are identified by the researchers – if a researcher finds a vulnerability and the company pays that researcher and then does nothing, or that flaw is publicized before it is fixed, the company can have security and liability problems.

The existence of the bug bounty program does not directly create a legal claim against the hacked company, but it is possible it could expose a company to a negligence claim especially if the flaws were both publicized and unaddressed.

To help mitigate that risk, companies should establish a robust process for using information that is submitted, and they should make sure the budget for the program includes not just money for researchers but for addressing any found issues quickly.

The company should not be collecting information that it is never going to act on. That would create potential legal risks.

In addition, you are paying someone for a service they are providing for you, so the legal risks are the same as they would be for other contracts.

CSLR: What terms should companies set for their bug bounty programs to avoid legal issues?

Yaeger: Companies should have the terms set as clearly as possible stating who is eligible to participate in the program, what bugs are eligible for submission, and what payments they will make for certain levels of problems identified. In addition, researchers should be told not to do certain things in the course of their research that could harm the company. For example, someone shouldn't try to do a denial-of-service attack to the company's website in order to test it. Also, a researcher should not engage in social engineering, which could violate the federal wire fraud statute.

The terms should make the scope of the program clear and make clear that the company is not endorsing that type of detrimental action. It is not that the company is necessarily preventing people from doing those things, but it is making clear those things are not authorized.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 7 April 5, 2017

[Editor's note: Facebook, for example, sets specific requirements one must meet to "potentially qualify for a bounty," including:

- adhering to the responsible disclosure guidelines;
- reporting a problem involving a product or service specified in a "bug bounty program scope" list and that is not in the excluded types of potential security issues;
- submitting the report through a specific form;
- using test accounts to investigate any issues; and
- disclosing any inadvertent privacy violation or disruption.]

CSLR: What is the risk if the company does not specify that certain acts are unauthorized?

Yaeger: If you leave open the possibility that something detrimental is authorized, it creates a potential issue, if for no other reason than you are limiting your own legal options and law enforcement's options to punish people who do bad things. It creates risks and potential liability if it's left ambiguous, whether or not researchers are permitted to undertake actions that really negatively affect the user experience on the website, the app, or other product. If the scope is clear and a researcher acts outside of the scope, there are legal actions that could be taken against the researcher.

[Editor's note: Facebook also specifies in its terms that certain things are outside the scope of the program, including "spam or social engineering techniques"; "denial-of-service attacks"; and "content injection."]

CSLR: Who should be eligible to participate in the program?

Yaeger: Companies should make employees ineligible to participate in the program. You don't want people to have an incentive to build code with vulnerability. Or, if you are using and testing software that was developed externally, you should specify that the researcher who submits the bug can't be the author of the vulnerable code. You wouldn't want the person who is developing the software to be the person selling you bugs.

Also, some of the researchers may be overseas, so companies should be aware of where their money is going and be aware of rules regarding payment of money to researchers in those countries. For example, the researcher you're paying should not reside in a country that is on a sanctions list. This includes the federal OFAC list, of course, but some U.S. states also have their own sanctions list for certain countries.

[Editor's note: For example, the Uber program terms specify:

> You are not eligible to participate in the Bug Bounty Program if you are: (i) a resident of, or make your Submission from, a country against which the United States has issued export sanctions or other trade restrictions (e.g., Cuba, Iran, North Korea, Sudan and Syria); (ii) employed by Uber Technologies, Inc. or any of its affiliates; (iii) an immediate family member of a person employed by Uber Technologies, Inc. or any of its affiliates; or (iv) less than 18 years of age.]

Some companies limit participants to a pre-selected group of researchers, which is similar to contracting with a vendor. For example, Apple recently launched its first bug bounty program and limited the submissions in the program launch to a small group of researchers it had worked with in the past.

CSLR: What type of confidentiality or non-disclosure requirements should be included in the program terms?

Yaeger: The program should be set up so that these secrets are given to you for you to act on them, and not simply dispersed into the world at large, which would largely eliminate the benefit you're getting. If you're paying people to find things and they announce them to the world at large, you don't get the running head start to fix the problem. Confidentiality provisions for the program should have clear terms that researchers should tell you this flaw and not others, at least for some set period of time. The program works if the researcher finds something out, tells the company, and does not tell other people, and then gets paid for it.

[Editor's note: For example, Facebook requests the following as part of its "Responsible Disclosure Policy": "We ask that: You give us reasonable time to investigate and mitigate an issue you report before making public any information about the report or sharing such information with others."]

CSLR: How should the bounty price be set?

Yaeger: It should be done in consultation with the technical team of the software maker who has a much better idea of the biggest risks. The companies have a lot of discretion in the payments. At the same time, it is important to have a clear contract, with clear terms describing the service and what the company is paying the researcher for. You wouldn't want to have unclear terms and then have people suing you for not paying a bounty.

And if you want to get the best people doing this, most likely you'll have to offer a higher price. Companies tend to tailor the bounties based on the severity of the vulnerability or based on the particular piece of software that is at risk. So something like a secure boot firmware component would be a lot more important (and thus would get a higher bounty price) than a more minor piece of code.

[Editor's note: PayPal sets a large price range: "The minimum bounty amount for a validated bug submission is $50 USD and the maximum bounty for a validated bug submission is $10,000 USD." PayPal will "determine all bounty payout based on the risk and impact of the vulnerability." It also specifies that there is no obligation for PayPal to pay a bounty and that if it "elects" to pay, it will make "partial payment when the vulnerability is first verified by PayPal and then an additional payment once the vulnerability has been fixed."

AT&T's payment terms are as follows:

> On a quarterly basis AT&T will evaluate all valid bug submissions that have been fixed (not reported) during that quarter and award bounties for what we consider to be the Top 10 Bugs or Bug Reporters for the quarter. Only bugs which represent a security risk to AT&T and its customers will be considered for an award; application functionality issues will not be considered. Only those Reporters included in the Top 10 will receive a bounty. The bounties range from $100 to $5,000 depending on the ranking of the Bug or Bug Reporter. AT&T will determine the Top 10 based on criteria such as the type/severity of the bug, impacted domain(s), potential bug exploits, and bug report submission quality.]

CSLR: Where would you advise companies to house these programs within the corporate departments?

Yaeger: There's no rule on exactly how you structure it, but it should be collaborative. Get a team together. This isn't going to be something that's done just by the legal side of your company and it's not something that's going to be done just by the technical or business side of the company. You need representatives from different units in the company to voice concerns and ensure that if the program is launched, necessary fixes identified will be implemented. It can't just be one person's initiative off to the side.

A lot of that is basic management and getting the firm to buy in. If you don't have enough buy-in and resources, you could be creating an issue by collecting information, putting yourself on notice and then not having adequate resources to fix the issue.

Before implementing the program, the team should consult with a company lawyer, but there's no per se reason that the program itself has to be housed in the legal department and I would be surprised if it were entirely housed in legal.

[See "T*ech Meets Legal Spotlight: Advice on Working With Information Security*" (Jan. 11, 2017) and "*How Cyber Stakeholders Can Speak the Same Language (Part One of Two)*," (Jul. 20, 2016); *Part Two* (Aug. 3, 2016).]