Bug bounty DIY: The pros and cons of managing vulnerability disclosure in-house

BY INTIGRITI · OCTOBER 4, 2023 · LAST UPDATED ON MARCH 6, 2025

So you've decided that your business or organization should launch a bug bounty program, a great first step in taking the leap into crowdsourced vulnerability reporting.

While choosing how and where to host your program can be an exciting time, the options can also become confusing and overwhelming. You might even ask yourself: can I just do it myself?

In-house bug bounty programs aren't unheard of, with the likes of Apple, Facebook and other big players in the tech industry choosing to employ a dedicated team to managing their own vulnerability disclosure environment. Other businesses or organizations choose to engage the services of a bug bounty platform, which can offer tailored support and management for their programs, allowing them to offer a bug bounty program without the need of an in-house team.

The bug bounty market is growing at a considerable speed, with the industry predicted to be worth more than $2600 million by 2027 – with no signs of slowing down. As the appetite for the market increases, as do the number of platforms offering the service, which can also become perplexing for organizations to choose which one, if any.

To help your business or organization come closer to understanding what works for you, we've compiled some of the pros and cons of what to expect when launching a self-hosted bug bounty program.

Pros

1. Fully bespoke

One of the reasons you might be considering building your own bug bounty program is to have a fully bespoke solution that your company or organization has full control of. You might want to be involved in every step of the process from deciding how and where you receive reports, to how and when these submissions are handled, right through to the finer details of how the bug fix is rolled out.

Running an in-house program means that you can not only have full autonomy over these decisions, but you can also change and adapt your program to suit you, dependent on your own timeline. For example, you might want to extend a private program to the public at the drop of a hat. Hosting your own program would allow you to do this, circumventing any restrictions or timescales you might face by using a third-party provider.

You might also want to host the program on your own website to maintain consistency with company branding and identity, or DIY might simply be in your nature, and the idea of starting a program from the ground up is something that excites you. Whatever the driver might be behind your decision, it's entirely possible to launch a homegrown bug bounty – and could be a fun project, too.

2. Potential cost savings

Probably the most obvious draw to running your own bug bounty program is that you don't have to pay someone else to do it. Sure, you might choose to pay a bounty (or offer swag as an incentive), but you won't have the added cost of paying a platform to oversee the program for you.

If time and resources allow it, you could even share the responsibility for maintaining the program across staff members or volunteers. Using voluntary staff is a great way to keep costs down for smaller businesses or organizations that don't have the budget to invest heavily in bug bounty.

You also don't need to provide a monetary reward for bug reports. Launching a vulnerability disclosure program (VDP) is virtually the same as a bug bounty, however VDPs don't offer a financial payout. You often find ethical hackers taking part in these kinds of programs even with the absence of financial gain – whether that's to learn new techniques, practice their skills, or simply to help keep the internet a safer place. You'll also find hackers drawn to VDPs to simply be a part of something bigger – in this instance, a little bit of swag and a shout out on social media can go a long way in attracting bug hunters.

Cons

1. Time consuming comms

Let's touch upon the potential downsides of running your own bug bounty program.

Maintaining one is time consuming, there's no two ways about it. While we might assume that the initial set up is the biggest drain on resource – and this can be significant – the day-to-day management of the program can actually become more involved than you might expect.

In an ideal world, the lifecycle of a bug bounty submission would look something like this: the bug is found and reported, the IT team receives the details, a patch is quickly and easily applied, and the issue is fixed. Unfortunately, this isn't always the case.

More complex bugs can't be fixed overnight and will need time and attention from the IT team. If the program is still accepting submissions during a phase such as this, a backlog of bug reports can quickly build up. Without a triaging team working specifically to identify the severity of bug submissions and prioritize them accordingly, this can potentially lead to the more serious of vulnerabilities slipping through the cracks, which could leave your company or organization exposed.

Bug bounty platforms offer an established triage team whose job it is to prioritize reports on behalf of organizations, responding to its community of hackers and keeping them engaged. This team will also manage communications with the researcher, so if any further information is needed this is taken care of, freeing the IT department to focus on the important task of fixing the issue at hand.

Without a dedicated team focused on maintaining a program, the signal to noise ratio can quickly become overwhelming. There are often a fair number of low quality or false positive reports that can take time to sift through, and in the absence of a triage team these kinds of submissions cannot be differentiated from others, meaning every report is potentially taken as a serious threat until it is proven otherwise.

2. Potential legal implications

One of the positives of running a public bug bounty program is that they invite ethical hackers from across the globe to participate, meaning you can gain access to some of the best bug hunters in the industry. It does, however, also come with some added due diligence to ensure that you're not falling foul of international laws.

Businesses and organizations must be compliant and avoid making payments to sanctioned countries, a list of which can be found on the **OFAC website**. In order to avoid making payments to unauthorized countries, they must verify that the person they're paying a bounty to doesn't reside in one of the sanctioned territories. This can be tricky to do for a company not specialized in this, not to mention time consuming.

One way of tackling this is to regularly and thoroughly check each participant's personal and banking information. Intigriti conducts daily OFAC screening ensuring that payments are not sent to unauthorized bank accounts. It also requires all bug bounty participants to undergo identity checks and conducts regular watchlist screening to ensure the people behind the username are exactly who they say they are.

The legal implications of paying an entity in a sanctioned territory vary depending on the details of the prohibition but could result in major financial penalties or criminal prosecution.

3. Tried and trusted model

Another downside to starting a program from scratch is that there is no tried and trusted model to work from. Bug bounty platforms specialize in helping businesses and organizations to crowdsource vulnerability testing, and so have a pretty solid idea of how to maximize a company's security posture no matter the industry, location or budget.

Intigriti has been doing so since 2016. Years of experience has also helped Intigriti to help its customers maximize their output from their program and make savings where it matters. For example, its **Bug Bounty Calculator** can help an organization to see whether the bounties they are offering are below industry average, and can also advise on what skill level of hacker its bounty levels are estimated to attract.

The calculator was built using anonymized data from more than 400 public bug bounty programs across 18 industries and is regularly updated to account for market fluctuations and other industry issues.

What should I choose?

Ultimately, that decision is up to you and the right answer can vary from organization to organization. Simply having any form of security reporting system is better than nothing and can go far in helping your business or organization to improve its security posture.

There are both positives and downsides to running your own bug bounty program, but with the right knowledge and investment of time and resources, any negatives can be minimized.

If you're interested in finding out more about how Intigriti can help you to maintain your bug bounty program, reach out to one of our team for details.