DIY or outsourced bug bounty programs: what's best for your business?

BY ELEANOR BARLOW · JUNE 24, 2025 · LAST UPDATED ON APRIL 2, 2026

What you will learn

- **How to decide between running a DIY (in house) bug bounty program or outsourcing to a specialist platform**, by weighing factors like expertise, legal support, and operational overhead.
- **How to set up an effective bug bounty program step by step**, including scoping, rules of engagement, budgeting, and measuring success for long term security outcomes.
- **How outsourcing to a bug bounty platform can reduce risk, streamline payment and triage, and improve researcher engagement**, helping maximise your program's return on investment.

Organizations are adopting bug bounty programs more and more as part of a layered security strategy to address the skills gap and to help their security budget go further. But should you run a program in-house or outsource to a bug bounty program provider? This blog will take you through the setup process and explain where the value from a bug bounty platform comes into play.

The right bug bounty program brings the following benefits:

- **Transparency:** Using a bug bounty program indicates that security is highly valued within the company, and that the company is prepared to participate with the ethical hacking community, not only to enhance security for their environments, but also for the benefit of their customers and partners.
- **Continuous testing**: Rather than a point-in-time test that can miss new vulnerabilities, bug bounty programs run nonstop and reduce real-world risk.
- **Skillset:** Access to security talent from across the globe, with diverse skills that most organizations can't get access to in-house.
- **Cost reduction:** Only pay for impactful results rather than the time it takes to run other, more traditional testing that may not produce results, that you still have to pay for!
- **Faster identification**: By having multiple researchers test environments simultaneously, gaps can be discovered faster.

INTIGRITI

Self-hosting a bug bounty program vs publishing via a bug bounty platform

Businesses can choose to receive and manage vulnerability disclosure reports themselves or publish and host through a bug bounty platform, such as Intigriti.

	SELF-HOSTED PROGRAMS	BUG BOUNTY PLATFORMS
Program engagement	**Reactive and passive engagement** Good-willed customers, citizens and ethical hackers will inform businesses of a potential security issue.	**Active engagement** Security researchers are continuously engaged through bounty opportunities, points and reward systems, leader boards, hacking events, education, and more.
Vulnerability disclosure policy requirements	**Required** Having a VDP ensures that people outside your organisation understand how to inform you of vulnerabilities they have discovered.	**Advised** It is advisable for businesses to have a VDP on their website too to direct people that wish to inform them of a security issue to their program.
Validating submissions	**Handled internally** Without enough manpower, the handling of non-valid submissions can be a time-consuming exercise.	**Handled by triage** Triage teams provide a layer of quality assurance before escalating vulnerabilities to businesses.
Handling comms	**Handled internally** Owned by the team tasked with fixing incoming submissions.	**Handled by triage** Communication carried out within the platform. A triage department works as the go-between for client & researchers.
Budget allocation & payment processing	**Manual** Responsibility of a finance department. To maintain good working relationships with researchers, it's important to provide payment promptly.	**Handled by the platform** Processes automatically after a submission is accepted by the organisation. Payment and administration are taken care of by the platform.
Disclosure agreement	**Responsible disclosure** Researchers encouraged to perform responsible disclosure via a VDP.	**Platform agreement** Researchers must agree not to disclose reports publicly unless given permission.

The good news? Planning and setting up your bug bounty doesn't have to be difficult!

How to plan your bug bounty program in 5 steps

Step 1: Scope

The first task to form your bug bounty program is to identify what needs to be included within the scope. Anything from APIs, mobile apps, web apps, or even certain hardware products can be included.

The second task is to identify and list all assets that are out of scope for analysis. This could include specific features or functionalities that a company might not want a hacker to access. Or perhaps it includes an area that was recently tested, so the budget would be better used elsewhere.

The third task is to decide if there are any specific vulnerabilities to search for. Different industries or regions can be susceptible to different types of attack, which makes a tailored approach better.

Working with a bug bounty provider, like Intigriti, provides an expert cybersecurity team that supports its customers and helps define scope, identify asset lists, and prioritize assets based on where a vulnerability could cause most damage, based on similar customer successes.

Step 2: Rules of engagement

In addition to your scoping document, you will need to create rules of engagement to highlight any techniques you don't want included. This could include elements such as attempts to gain unauthorized access, attempting a data breach, or causing disruption.

'By default, researchers from the Intigriti platform are bound to certain rules. For example, researchers cannot use methods of DDoS attacks or social engineering; they must disclose vulnerabilities immediately and cannot disclose information without written consent in the platform. It can be useful to add some restrictions to explain how you expect researchers to behave and what they can expect from you.' – ***Rules of Engagement and Testing requirements.***

Be sure to strike a balance of openness with protection. You don't want to stifle the work of the ethical hackers, but you equally can set parameters to prevent them from delving into elements you don't want tested.

Step 3: Program policies

Putting in place comprehensive terms and conditions and making elements such as SLAs, submission guidelines, communication, and disclosure rules clear is paramount to avoid any legal issues that could arise. Partnering with a bug bounty platform provider removes the burden of setting up legal frameworks yourself, offering established, robust legal structures that account for varying locations, jurisdictions, and company policies.

Step 4: Budget

Setting a concrete reward structure for your bug bounty program is very important. Why? If the researcher finds a critical or exceptional vulnerability but is not paid fairly for the find, they're likely to disengage.

Set different severity levels and impact of a reported vulnerability into a tiered system so that all bugs found are rewarded fairly.

Clearly define how and when payments will be made, to save any confusion or doubt, and be completely transparent with your ethical hacking team.

Many customers turn to bug bounty providers to set up safe, fast payment processing for the researcher. This ensures payment is made in days rather than weeks/longer. When companies try to pay an ethical hacker directly without the KYR (Know Your Researcher) screenings in place, this can lead to slower processing of payments, which often leads to lower engagement.

'In an analysis of bug bounty programs, a trio of academic researchers concluded that the programs were cheaper to run than hiring expert security researchers to find software vulnerabilities. Vulnerability rewards programs can range anywhere from two to hundreds of times more cost-effective than hiring expert security researchers to find vulnerabilities.' – SecurityWeek.

Step 5: Measuring success

Measure the success of your bug bounty program by monitoring KPIs. These can include tracking statistics like:

- The number of valid reports
- The number of reported vulnerabilities
- The average response time (how long it takes your team to respond to highlighted vulnerabilities)
- The number of payouts and the frequency of payouts

Regularly review and adapt processes so that the scope, reward structure, and processes are as effective and relevant as possible. By keeping tabs on the challenges faced, it will make it clearer when to expand or contract the scope, raise or lower boundaries, and relax or tighten rules.

Intigriti's streamlined, bespoke reporting is built for our customers' needs, to supply reports and data to enhance their visibility and simplify actions.

Next steps and considerations

An effective bug bounty program requires both strategic and technical effort to understand organizational security priorities, scope, and structures. It also requires consistent communication and education to build trust with ethical hackers and keep them engaged

Consider what you want from your bug bounty program, and make sure to look for a platform that offers the following elements:

- Active and engaged hackers
- Easy communication
- Payment gateway integration

Bühler, a Swiss multinational plant equipment manufacturer, known for services for processing foods and manufacturing advanced materials, highlighted that

> **"By using Intigriti bug bounty, it streamlined the entire compensation process, alleviating Bühler's legal and administrative burdens by managing payouts and necessary identity checks.**
>
> **- *Exploring Bühler's strategic collaboration with Intigriti.* "**

Also look for:

- A robust triage process and validation of reports. For more information regarding the impact of triage when setting up your bug bounty program, read this blog.
- Developer collaboration for patching.

When executed correctly, a bug bounty program can significantly strengthen defences. But success will depend on a balance between security, engagement, and transparency. Keep goals clear-cut, guidelines firm, and communication open.

> **"Given the complexity of systems, protocols, and experience required, as well as the amount of time needed for good triage, the best approach to running an internal bug bounty program is almost always through a dedicated bug bounty platform, like Intigriti. You get the best of all worlds: a fun, educational program; improved cybersecurity; and the time-consuming process of triage handled by experienced experts."**
>
> **Pascal Schulz, Team Lead Solutions Engineering, Intigriti**

For more tips and tricks on how to implement your bug bounty program, reach out to the team here.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.