The major bug bounty debate: Which department should pay for rewards?

BY ANNA HAMMOND · JANUARY 18, 2024 · LAST UPDATED ON MARCH 6, 2025

When launching a new bug bounty program, there's usually a discussion around which department should 'foot the bill' for the costs of the rewards. It's for that reason many clients turn to Intigriti to understand the norm. The truth is, however, there is no universally agreed-upon standard regarding which department should take charge. Moreover, there are genuinely tangible advantages for some teams to assume ownership of bounty costs.

On-demand webinar! Money Talks: Optimize Your Security Testing Budget To Drive Maximum Value

So, how do you navigate this decision-making process and choose what's best for your organization? In this article, we will break down the essential factors to consider when making that decision.

The size and scale of an organization will impact bug bounty reward responsibility

Departmental budget responsibility for budget bounty spend varies greatly depending on the size and scale of the organization running the program. For example, in many cases, it comes directly from the security team's budgets. In other cases, organizations believe it should be funded by the product and engineering teams that own the affected asset. Legal, risk and compliance teams can also pick up the tab in less common cases.

Speaking directly to Intigriti's Customer Success Manager, Harry Prestwich, we asked which scenario works best in his experience.

"There is no definitive answer regarding the source of the budget. However, in my experience, the most effective approach is when the security team takes ownership of the investment while the budget for bounty rewards is allocated among the product teams responsible for each affected asset. This arrangement proves successful as it establishes the groundwork for a product development life cycle that prioritizes security."

The advantages of allocating bug bounty reward costs to product and engineering

Javvad Malik, Lead Security Awareness Advocate at the Security Training organization KnowBe4, brought forward another perspective on determining the allocation of bug bounty spend. He explains, "Security teams usually have a budget for pentesting, which is traditionally done pre-launch without risk exposure, and any issues can be fixed easily. But bug bounties can have a long tail, and it isn't really feasible for a security team to budget for them."

At first glance, it may appear unfair for the product and engineering teams to shoulder the burden of bug bounty rewards while the security team takes ownership. However, there is a compelling rationale behind this approach to budget allocation.

Here's three significant benefits of this setup:

1. It leads to security-minded Product Developers

In many developer education programs, security principles are often overlooked. However, when product and engineering teams are responsible for funding approved vulnerability rewards, it incentivizes the business to prioritize educating development teams on mitigating vulnerabilities and risks.

2. Awareness increases around the ever-evolving cyber threat landscape

The lack of education in this area also leads to limited awareness among developers regarding the ever-evolving cyber threat landscape. Intigriti's platform provides genuine demonstrations of the expanding threat landscape. Engaging the product and engineering teams directly through their financial backing is a proven way of achieving greater awareness in this area.

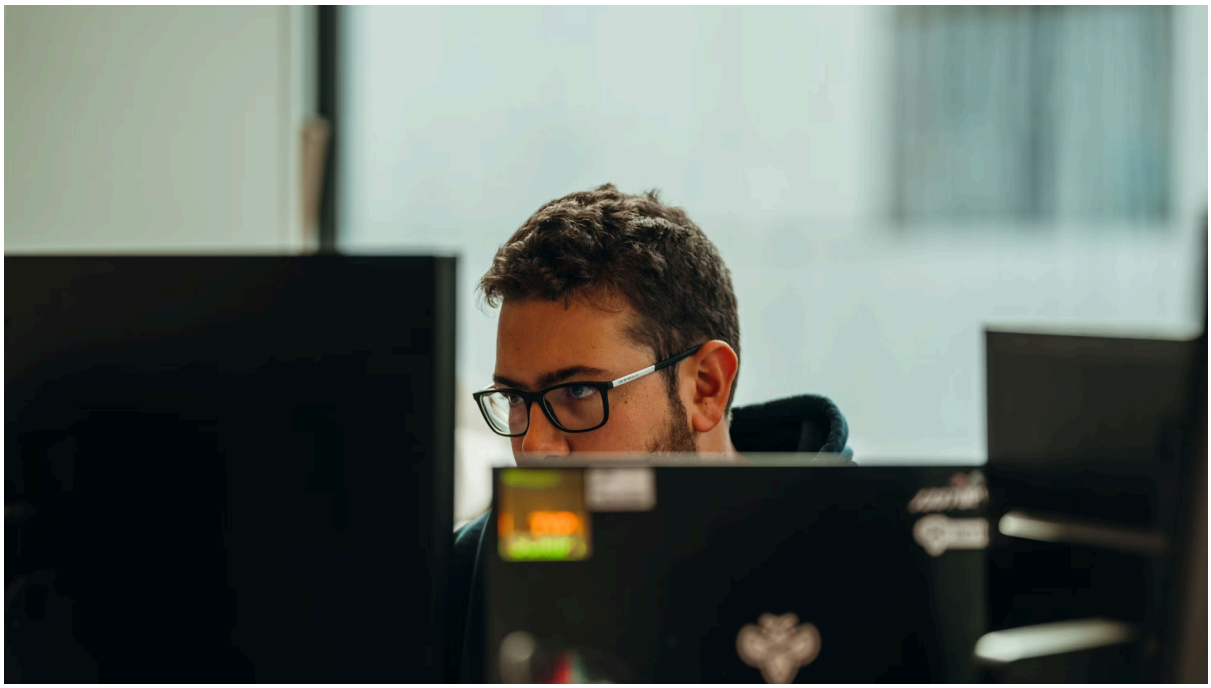
Yash Gorasiya, Associate Project Manager at pentesting exam provider The SecOps Group, agrees that having financial obligations sit with the product and engineering team increases cyber threat knowledge. He explained: "With basic security education becoming part of their training routine, it's crucial to focus on identifying loopholes that may arise during product development."

3. Financial obligation drives change

When product and engineering teams witness the costs associated with mitigating vulnerabilities within their budgets, it often serves as a catalyst for positive change. This financial obligation drives teams to reassess their development and deployment strategies.

Navigating third-party perils when allocating costs

Assigning responsibility for bug bounty payouts may appear straightforward, especially when the product team is accountable for the code that introduced the security vulnerability. However, what happens when they didn't? Complications arise when third-party code or dependencies are involved, potentially introducing vulnerabilities if insecure code goes unchecked. Should the responsibility for bug bounty rewards fall on the other party in such cases?



The answer is both yes and no. When launching a bug bounty program, companies establish boundaries that stipulate what is in and out of scope. Often, companies will explicitly list third-party vulnerabilities as out of scope for rewards, meaning ethical hackers may not receive financial compensation if the vulnerability is not directly attributable to the software manufacturer.

Gorasiya remarked: "If we talk about a third party [bug] affecting the company, then it would depend on the kind of agreement the parties had during the time of collaboration." Nevertheless, there are instances where companies choose to pay out for third-party security vulnerabilities. Gorasiya cited cases in which security researchers have been paid rewards from Google and Facebook (now Meta) for submitting bugs in third-party websites or applications that use Facebook data.

In a statement, Meta explained their rationale for paying out on some third-party bugs, stating, "Although these bugs aren't related to our own code, we want researchers to have a clear channel to report these issues if they could potentially lead to the misuse of our users' data."

Maximizing the value of your bug bounty budget and justifying the investment

At Intigriti, our goal is not to burden companies with continuous spending on fixing common vulnerabilities. Instead, we strive to help companies reach a point where the number of valid vulnerabilities discovered on our platform stabilizes or decreases as they mature in terms of security. One of the most effective ways to achieve this is by using each vulnerability found as an opportunity to prevent its recurrence. It's not just about discovering vulnerabilities; it's also about educating and improving security practices.

Companies with mature security postures often adopt a strategy that assumes they will be targeted by hackers and then work backwards to mitigate that risk. With an increasing media focus on security incidents and malicious hacks, numerous high-profile cases have made headlines worldwide in recent years. This prompts an important question: "How much would a company be willing to invest to avoid becoming the next headline news story about a major security breach?

If you want to speak with someone at Intigriti about optimizing your budget for your bug bounty program to drive maximum value, get in touch.