Bug bounty ROI: Can investing in crowdsourced security help mitigate costly security breaches?

BY INTIGRITI · APRIL 12, 2024 · LAST UPDATED ON APRIL 8, 2025

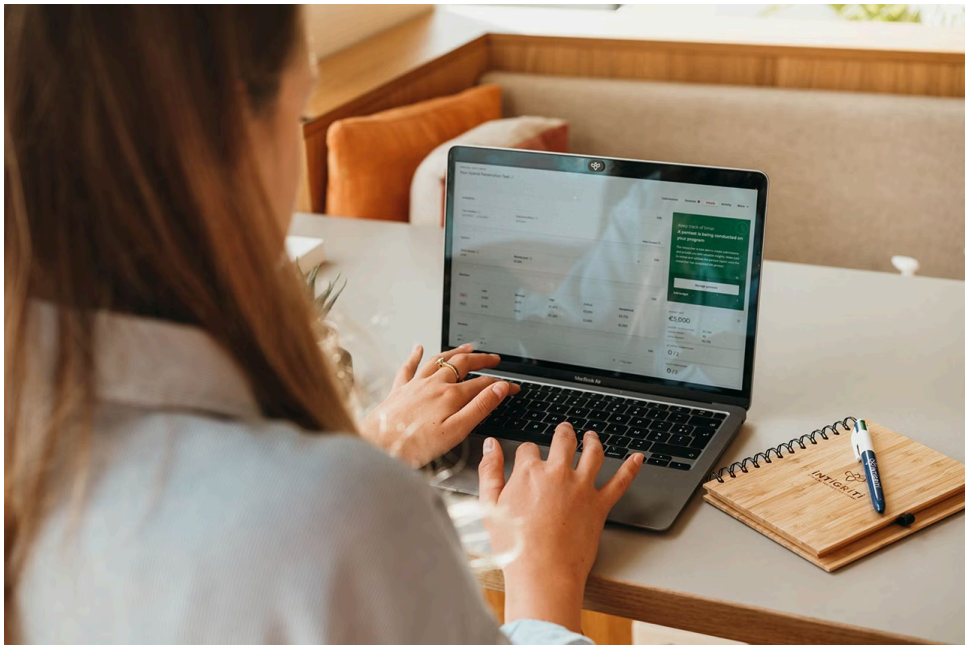
Factoring in whether to allocate resources for a bug bounty program in your annual cybersecurity budget can be a challenging decision. In comparison to alternative strategies, bug bounty programs offer a proactive approach to bolstering digital defenses. However, assessing the true return on investment (ROI) of such programs requires a thorough examination of their benefits and costs.

Despite the initial investment, bug bounty programs offer substantial potential cost savings. The expenses associated with a security breach far surpass the upfront costs of implementing proactive security measures, as we'll delve into later in this article.

It's also worth noting that cost of implementing a bug bounty program can vary significantly between businesses, influenced by factors such as the organization's size and specific requirements. Larger enterprises may need to invest up to $250,000 for comprehensive coverage, while smaller businesses can establish effective programs for as little as $35,000.

In this blog, our aim is to guide you in understanding which solution is the right fit for your organization. To provide context, let's first explore the average cost of another valuable security testing tool: pentesting.

The average cost of a pentest



A popular alternative to using bug bounty is to commission regular—often annual—penetration testing. Penetration testing, often referred to as "pentesting," is a service that companies commonly outsource to third-party security experts. During a pentest, the pentester thoroughly scans the organization's networks and systems to identify potential security vulnerabilities. They then generate a detailed report of their findings, frequently including recommendations for mitigating the discovered vulnerabilities.

On average, a pentest can cost between $15,000-$30,000, though the cost can depend on the parameters of the test. Tight budgets can mean that an extensive report isn't financially viable, so in this case, the pen tester might do a 'light touch' test. The insights of a pentest are also dependent on the knowledge and skills of the individual carrying it out, so there is potential to miss bugs that require a certain set of skills or deeper investigation.

Pentesting ROI

While a pentest can be a great way for companies to assess their security posture, this point-in-time assessment may miss vulnerabilities that continuous testing can pick up. In fact, in our Ethical Hacker Insights Report we found that of those polled that had hands-on pentesting experience, 88% agree or strongly agree that "a penetration test cannot provide continuous assurance that an organization is secure year-round."

Speaking on this, Intigriti's Chief Hacker Officer Inti De Ceukelaire said: "Penetration tests focus on one snapshot in time, whereas bug bounty programs are continuous. As attackers shift tactics, cyber defenses must too. The only way to test their effectiveness is to apply continuous pressure against them. Considering that an organization's security posture will change with each new feature release or update, it's not only a logical step to implement more security testing, but also critical."

Just 14% of the pentesters also believed that a penetration test would be able to find all of the same types of vulnerabilities they have found during bug bounty hunting.

Things to consider when weighing up bug bounty ROI

Now, let's move on to the heart of the matter: bug bounty programs. Here are the key things to consider when assessing their ROI and weighing up your alternative options.

1. The cost of an internal security team

It can cost more than $456,000 a year on average for a business in the US to employ a competent security team to protect its networks from vulnerabilities. This is based on the average annual salary in 2023 of three security researchers (around $91,600 in the US) plus an additional $182,000 for a head of security, according to Indeed.

A study from researchers in the UK also reported that it was "economically viable to run bug bounty programs instead of hiring additional researchers". The paper's authors argued that considering average payout fees, report cadence, and other costs associated with hosting a bug bounty program, the average annual cost of the programs included in the paper is around $84,000. Compared to the potential cost of hiring a security team, the researchers noted that bug bounty was a preferable option for some businesses or organizations – especially those concerned with sticking to a budget.

This figure will vary depending on the specifics, such as the level of support required for the program and the platform it is hosted on. However, it gives an indication of the potential cost savings associated with having a bug bounty program rather than solrely relying on an internal security team.

2. Savings on cyber insurance premiums

Investing in proactive security measures, such as a bug bounty program, can also help save money on potential costly cyber insurance premiums.

These days, it's normal practice for businesses and organizations to be insured against the risk of a cyber-attack—and as the rate of cyber intrusions rises, the cost to protect against them also increases. The Global Insurance Market Index from Marsh estimates that spending on cyber insurance rose by 11% in Q1 of 2023, and a further 1% in Q2.

As the frequency and severity of cyberattacks continue to rise, insurers are increasingly incentivizing organizations to implement robust security measures. By demonstrating a commitment to cybersecurity, organizations can negotiate lower insurance premiums and reduce their overall risk profile.

3. The cost of a breach

The financial repercussions of a security breach extend far beyond immediate remediation expenses. From regulatory fines to reputational damage, the fallout from a breach can be catastrophic. The average cost of a data breach in 2024 exceeded $4.88 million, whereas the average bounty for an exceptional or critical vulnerability found through the Intigriti bug bounty platform is $6000. That means that the average bounty is less than 1% of the average cost of a malicious breach.

Jarno Vanlerberghe, Customer Success Manager at Intigriti, shares some personal insight on data breaches and bug bounty ROI:

"One of our customers in the retail industry only invested about €12k in bounty budget over two years, but our community discovered multiple critical and exceptional vulnerabilities that could have led to millions in data breach costs. More specifically, the average cost of a data breach in retail is more than €2.7 million. This is exceptional ROI."

4. The price of handling media relations after a breach

The aftermath of a security breach extends far beyond technical remediation efforts, often requiring a substantial investment in managing media relations. When a breach occurs, organizations must navigate a complex landscape of public scrutiny, media inquiries, and reputational damage control.

Lucia Barbato, CEO at Ilex Content Strategies, told Intigriti: "As well as having potential legal implications, a security breach can impact the level of trust that a brand enjoys. Trust can take years to establish and moments to erase. Brands must therefore be seen to be taking an open, honest and proactive approach should a situation like this arise."

On how much a security breach can cost a company financially, Barbato said that it "is almost impossible to quantify." Barbato added: "It depends on the level of the breach, the organization involved and how it came about. The loss of trust is unquantifiable, and bringing in a PR team won't be a quick fix. Often these relationships are long term. Trust is cumulative—once the immediate crisis recedes, the rebuilding will take time."

5. The cost of regulatory fines

The cost of regulatory fines stemming from a security breach can impose significant financial strain on organizations. Regulatory bodies worldwide impose hefty fines on companies found in violation of data protection laws and regulations.

For instance, the European Union's General Data Protection Regulation (GDPR) enforces fines of up to €10 million or 2% of a firm's worldwide annual revenue, whichever is higher. Similarly, regulatory agencies in the United States, such as the Federal Trade Commission (FTC), have the authority to levy penalties on businesses that fail to adequately protect consumer data.

By investing in bug bounty programs and implementing robust security measures, organizations can minimize the risk of regulatory fines and protect their bottom line.

Is a bug bounty program worth the investment?

By proactively identifying and remedying vulnerabilities, organizations can minimize the financial risks associated with security breaches.

While the initial investment may seem daunting, we believe that the long-term benefits far outweigh the costs.

Get in touch with the Intigriti team to find out more about investing in your own program today.