Building a case for bug bounty programs: Addressing corporate concerns

BY ANNA HAMMOND · APRIL 3, 2024 · LAST UPDATED ON MARCH 6, 2025

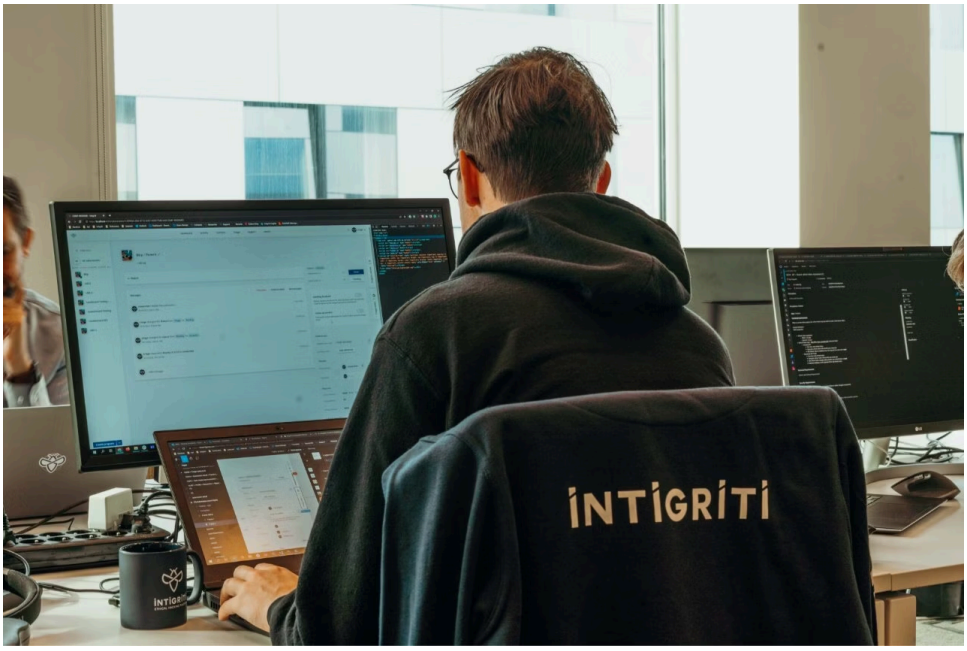
Bug bounty programs have emerged as a powerful tool in the cybersecurity arsenal, empowering organizations to proactively identify and resolve vulnerabilities before they can be exploited. Despite this, internal concerns around financial implications, legal complexities, data security risks, and cultural barriers can hinder the adoption of these programs.

Companies needn't be afraid to step into the world of bug bounty programs. This comprehensive guide aims to address concerns head-on, empowering organizations to build confidence in bug bounty programs and unlock their full potential.

Let's jump in with the most common questions and concerns security teams are met with when building a case for a bug bounty program.

Tip! Want to get to grips with the basics of bug bounty programs before we dive into this topic? Simply head to this page and become an expert!

Dispelling doubts around ethical hackers



Bug bounty programs provide organizations with a valuable tool to identify and address security vulnerabilities. However, some organizations hesitate to embrace these programs due to concerns about data security and the potential misuse of sensitive information. These concerns are understandable, but they can be effectively addressed with some of our responses below.

1. Aren't we putting ourselves more at risk by opening ourselves up to hackers?

The unfortunate truth is that bad actors won't seek permission before targeting your business. To outmanoeuvre cybercriminals, the key is to beat them to the punch. Bug bounty programs are designed with this goal in mind, empowering companies to simulate real-world threats in a controlled environment through the power of thousands of security-driven professionals.

However, a question often arises: Can we trust these individuals, especially when we don't personally know them? Does allowing anyone to "attack" us expose us to more risk? The answer is simple: **yes, you can trust Intigriti's community.**

Intigriti has undergone rigorous international standards to ensure the overall security and integrity of the company. As part of this security framework, researchers cannot participate in bug bounty programs anonymously. All 90,000+ ethical hackers currently on our platform, as well as future hackers, sign terms & conditions (T&Cs) and undergo an ID check by Intigriti before accessing the platform. Let's delve into this further.

Researcher T&Cs

Intigriti's community sign-up process ensures that every ethical hacker (also known as security researchers) has read and accepted the legally binding researcher T&Cs, which include strict guidelines on confidentiality, data processing, non-disclosure of vulnerabilities, and more. Once accepted, an Intigriti Community Code of Conduct becomes applicable too.

ID checks

Security researchers must also undergo Intigriti's identity verification process, which includes checks for fraud, stolen IDs, and impersonation.

By implementing these stringent measures, Intigriti ensures that trust and security are at the forefront of our bug bounty programs, providing peace of mind to organizations seeking to enhance their cybersecurity posture.

2. We're not ready for 90,000 hackers to test our security posture

We get it—opening yourself up to 90,000 ethical hackers as your first introduction into the world of bug bounty programs is daunting. It's for that reason that, when new to crowdsourced security, we suggest that organizations generally start with a private program.

Each program on our platform has its own dynamics and level of openness to the security community. For those taking their first steps, we recommend starting with a private bug bounty program. A private program is a great first step for organizations wanting to dip their toe into bug bounty programs without too much initial exposure. They're invite-only and don't appear in public listings.

Private programs are beneficial when you need to focus on a particular area of technology, such as splitting out your web apps, mobile apps or infrastructure. Intigriti's Solution Architect, Amar Chavda, explains why:

“Organizations can define the required skillsets and specialisms they need and then we can invite researchers who meet these criteria to participate in their program. We’ve also observed some clients using multiple programs for organizational purposes, such as having a dedicated program per team to manage responsibilities internally.”

Private programs are also well-suited to decentralized security teams. For example, splitting subsidiary company into individual programs and assigning them the appropriate team to manage and test their own assets.

Another option for organizations is to publish a public program that requires researchers to apply to participate. Application Programs are visible just like a public program, however, with limited information provided. For instance, a description and a bounty level are shown, but researchers need to apply to join these programs. If accepted, the remaining details are then disclosed.

Conquering cost concerns about bug bounty programs

At Intigriti, we know that bug bounty programs offer a compelling financial advantage for organizations. However, unlike some core business components, such as HR software, bug bounty programs aren’t commonly known within the wider business. Naturally, questions arise about the necessity of bug bounty programs and how organizations can ensure a return on their investment. We’ve addressed the most common concerns below

3. How can we justify the additional cost of a bug bounty program?

The financial impact of a single data breach can be substantial, encompassing legal fees, forensic investigations, regulatory penalties, and customer compensation. Further still, remediation efforts caused by a security breach are often time-consuming, expensive, resource-intensive, and disruptive to business

operations. By proactively addressing vulnerabilities, organizations can prevent potential attacks, minimizing the risk of data loss, system downtime, and operational disruptions.

Moreover, in the event of a successful cyberattack, it isn't necessarily the CISO who is going to be held accountable in the eyes of the public. One notable example of this is the TalkTalk data breach in 2015. The then-CEO, Baroness Dido Harding, found herself on the front-line facing probing questions from the media about what had occurred and how she had allowed it to happen under her leadership.

Interview with then-CEO of TalkTalk, Baroness Dido Harding

Discussing her learnings from the event, which cost the telecommunications provider £400,000 and led to Harding's eventual resignation, the former CEO said: "The first big teaching that can be drawn from this is the need for the board to ask IT and Security teams the right questions. Is the cybersecurity plan good enough? Are systems physically okay? What is causing you concern regarding network security? Without the board asking these questions and advocating for responsibility from the top, organisations will not be able to effectively mitigate risk. The second big lesson that from the TalkTalk data breach was that cybersecurity is definitely a board responsibility."

4. Why do we need another security test?

When putting together a business case for your bug bounty program, you may be met with: "We already spent a lot on the penetration test you requested. Why do we need additional tests?"

Traditional penetration tests tick a lot of boxes, such as helping meet compliance standards. However, pentests depend on an assessment that is performed at a specific point in time, meaning risks could go undetected between evaluations. Bug bounty programs, on the other hand, offer ongoing protection against malicious hackers.

Using pentests and bug bounty programs together makes for a powerful combination, significantly reducing the risk of a successful cyberattack occurring.

5. Why not invest in our internal security team instead?

The more you can invest in your internal security team, the better. However, for many organizations, growing the team isn't always an option—or even necessary. Fortunately, bug bounty platforms, such as Intigriti, are powered by crowdsourced security, meaning organizations can leverage the expertise of a global cybersecurity community through a single platform. Intigriti, for example, has 90,000+ ethical hackers within its community, offering a diverse range of skillsets and backgrounds.

By engaging a diverse pool of external security researchers, organizations can access a broader range of expertise and perspectives without adding to their headcount. This cost-effective approach allows organizations to enhance their security posture without straining budgets.

6. How can we maintain control of what we spend?

For those unfamiliar with bug bounty programs, a common concern is the potential waste of budgets on irrelevant vulnerabilities. This concern extends to the potential for costs escalating out of their control. Rest assured, Intigriti's platform removes the potential for these events through several key measures.

Below, we give four examples:

Triage

Perhaps the most crucial aspect is Intigriti's commitment to delivering only relevant vulnerability reports through our platform. You have full control over the scope of your bug bounty program, clearly defining what should be tested and what shouldn't. Our in-house triage service, included with all programs, ensures that you receive actionable and valid reports. This comprehensive service handles researcher communications, validates vulnerability reports, reproduces issues, provides proof of concept, describes the impact, and offers recommended solutions when available. Additionally, we proactively follow up with companies to address any missed or misunderstood reports, providing further assistance on how to take appropriate action.

Program confidentiality levels

Organizations have **different levels of openness**—offering organizations more flexibility and control over their programs than simply being private or public. The level of visibility of a program influences the degree of control organizations have over researchers participating in the initiative. This, in turn, impacts the number of submissions and the total expenditure on bounties.

Spending limits

When you launch a bug bounty program with us, you can set a spending limit. Once this limit is reached, the program automatically freezes, preventing any further submissions. This ensures that you never exceed your budget, allowing you to sleep soundly at night knowing that an unexpected bill won't catch you off guard when you wake up!

Dynamic pooling

Customers on our advanced plans can also take advantage of the Dynamic Pool feature. This intelligent system dynamically manages allocated budgets for programs, drawing from the unallocated pool as needed. By simply adding funds to the unallocated pool, programs can access the necessary budget, preventing them from entering auto-suspension.

These measures, among others, empower organizations to maintain complete control over their bug bounty program and security testing budget.

Demystifying the legal and data security complexities of bug bounty programs

Bug bounty programs involve complex legal and data security considerations that organizations must carefully address to ensure compliance and mitigate potential risks. Understanding these complexities is crucial for building confidence in bug bounty programs and reaping their full benefits. Here, we'll aim to cover how Intigriti can address these questions and concerns.

7. How can we ensure our data and that of our customers remains secure?

Intigriti is fully compliant with GDPR, as you can read here. Our platform also offers unique data-protecting functionalities, including the option to permanently delete submissions, strong encryption measures, PII detection flags in reports, and the ability to restrict program access in certain regions. Top tech companies have selected Intigriti for its exceptional security measures implemented on our platform.

Turning skeptics into supporters and driving the benefits of bug bounty programs

Bug bounty programs offer organizations a powerful tool to proactively identify and address vulnerabilities, bolstering their cybersecurity defenses. More and more cybersecurity leaders and professionals are embracing the power of crowdsourced security testing—but convincing internal stakeholders of these benefits is still a challenge for many.

At Intigriti, we understand the importance of addressing these concerns head-on and providing comprehensive solutions. Our platform offers robust security measures, including strict researcher terms and conditions, identity verification processes, and control over program budgets. We prioritize trust, transparency, and collaboration to ensure a successful bug bounty program.

If you're ready to take the next step and harness the power of bug bounty programs, you're in the right place. We're here to guide you through the process, answer any questions you may have, and help you build a strong case for crowdsourced security testing. Together, let's strengthen your defenses and stay ahead of evolving threats. Get in touch with us today.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com