How to get the most out of your cybersecurity testing budget

BY INTI DE CEUKELAIRE · FEBRUARY 8, 2024 · LAST UPDATED ON APRIL 16, 2025

How security professionals can achieve more with less

The responsibilities of CISOs and other security professionals are growing more complex. As cyber threats escalate, organizations must defend themselves within tight budget constraints, making crafting an adequate cybersecurity budget paramount.

A well-structured budget not only tackles immediate threats but also establishes a foundation for future-proofing against evolving cyber challenges. This article emphasizes the crucial steps that CISOs mustn't overlook to maximize the value of their investment.

How to achieve more with your cybersecurity budget

Let's dive into some of the ways you can achieve even better results from the cybersecurity budget you do have.

1. Assess your existing cybersecurity posture

Testing your security posture is a good way to know the effectiveness of your existing cybersecurity efforts, which is often achieved through security testing tactics.

At Intigriti, we encourage our customers to do a pentest with us first so that they can assess their maturity before committing to anything further. This step prevents you from potentially spending your cybersecurity budget on activities that you're not ready for yet.

2. Security testing: pay for value, not just time

Diversifying your cybersecurity testing approach is a key strategy for achieving more with less. Instead of solely focusing on just one method, consider adding other approaches into the mix.

When you rely on pentesting alone, you're paying for the time of the tester (regardless of the results they produce) and a snapshot view of your company's security posture. While that may give a good indication of your security posture at that moment, the solution doesn't help you to stay alert to new threats. It also won't identify future vulnerabilities that emerge in your systems and assets.

On the other hand, if you spend some of your budget on a bug bounty program, you'll pay for both results and time – and you'll benefit from enhanced security coverage because it's ongoing.

In an ideal scenario, organizations should split their cybersecurity testing budget between bug bounty programs, penetration tests, and responsible disclosure. This holistic approach ensures comprehensive coverage and encourages proactive identification and remediation of security flaws.

3. Employee training and awareness

Don't forget to set a little budget aside for internal cybersecurity training. Even if you can spare just a small amount, increasing internal awareness will pay dividends in preventing security incidents and minimizing the likelihood of human error-related breaches. Consider investing in simulations to test employee competence and work out where the weak spots are. Once you have the results, you can tailor an educational program to roll out.

4. Invest in crowdsourced security

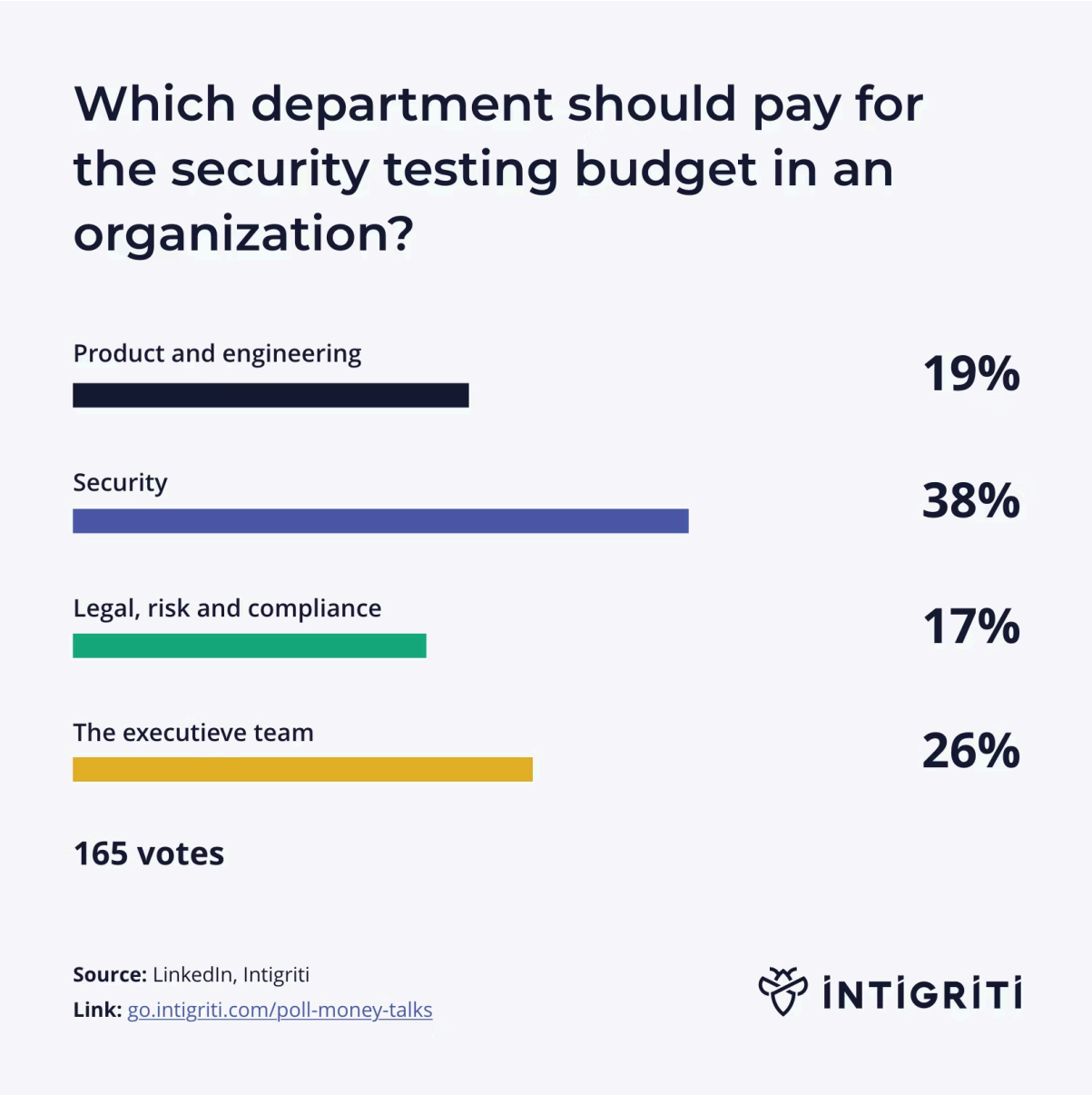
To really get the most out of your cybersecurity budget you may want to explore the concept of crowdsourced security. By connecting with a global community of talented security researchers, organizations can leverage real-time insights and continuous testing.

When companies spend their budget on pentests alone, they're relying on a singular researcher (who is being paid regardless of the results they find) to uncover vulnerabilities within a limited timeframe. This provides only a partial view of their overall security posture, at a single point in time.

On the other hand, crowdsourced security is agile, cost-effective, and provides a dynamic approach to staying ahead of emerging threats. Rather than relying on just one researcher, you can access a global pool of motivated, talented ethical hackers to spot vulnerabilities and help you stay ahead of threats.

So, which department should the bug bounty budget come from?

The question of which department should cover the bug bounty reward budget is one we're met with a lot. Unfortunately, there's no black-and-white answer to this, as is illustrated by the varying responses we received from our own community.



However, we do have a 'best practice' approach that our Customer Success team see working effectively across many organizations:

"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." *Harry Prestwich, CS Operations Manager at Intigriti.*

By sharing the ownership of this cybersecurity investment, companies often find that a greater awareness of security best practices develops across teams.

Measuring ROI and demonstrating value from your cybersecurity testing budget

Measuring ROI is paramount when it comes to justifying your budget to key stakeholders and demonstrating the value it brings. It's also important for you to see if you're really getting the most for your money.

While it can be challenging to quantify the value of prevention, there are several metrics you can use to showcase the effectiveness of your cybersecurity testing initiatives.

Firstly, assuming vulnerabilities are discovered and addressed, assess the improvement in incident response time and efficiency. Measure the time it takes to detect and respond to security incidents after implementing updated cybersecurity measures. A decrease in response time indicates improved security posture and reduced potential damage.

You can also think about compliance considerations when it comes to demonstrating value. Ensuring compliance with legal frameworks through continuous security testing not only mitigates the risk of fines but also fosters trust and confidence among customers and partners – making it a huge value add.

Other considerations include internal levels of security awareness before vs after, or how many vulnerabilities are found in pentesting vs how many are found in bug bounty. Ultimately, it's down to you to choose which factors you should measure to demonstrate the most value to your stakeholders.

Final thoughts: crowdsourced security is key

Getting the most out of your cybersecurity testing budget requires strategic planning, effective resource allocation, and continuous evaluation of ROI. But most of all, it requires diversification. By diversifying your cybersecurity testing and opting for a crowdsourced approach, you can rely on a global pool of talented researchers to help you stay abreast of risks on an ongoing basis.

To get even more insight on this topic, watch our on-demand webinar here.