Bug Bounty Programs Are Not a Quick-Fix

WHAT'S INSIDE

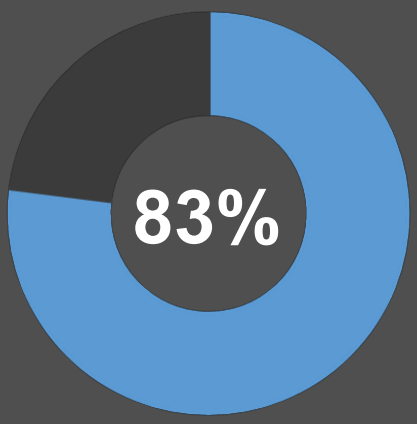
- Vulnerability Awareness
- The Truth About Bug Bounty Programs
- Focusing on Development + Testing Phase
- Need for Proactive Layered Approach

WAKEFIELD

Introduction

QuickStats
83 percent of respondents have released code before testing or resolving issues for bugs

ITDMs in Cybersecurity



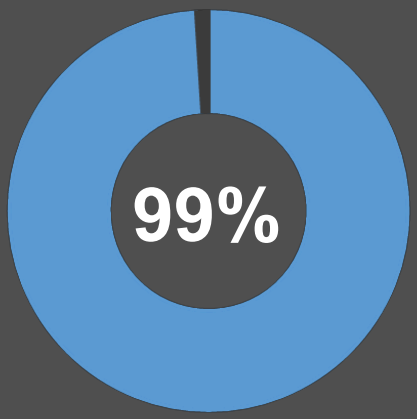
There is an urgent need for improved detection and vulnerability awareness in today's threat landscape. Whether it makes headlines or not, every cyberattack is further evidence of the gaping hole in securing business software. Many organizations lack the proactive, layered security programs necessary to combat today's vulnerabilities. What's worse, many IT professionals are feeling a false sense of security, specifically as it relates to the secure state of their applications. In an effort to learn more about the current perception of application security techniques, inclusive of the much-hyped about bug bounty programs, IT decision-makers were surveyed by Wakefield Research for Veracode. The data produced further signified a few things: organizations must educate themselves more on the importance of application security programs and bug bounty programs are not the end all be all quick-fix solution some organizations think they are.

According to the survey data, although 99% of respondents feel as though their organization's software and applications are secure, 83% have admitted to releasing code before testing or resolving security issues for bugs. These numbers beg the question: "How can an organization be considered secure if proper security measures are not applied to critical components of their business, starting at the application layer?"

Vulnerability Awareness

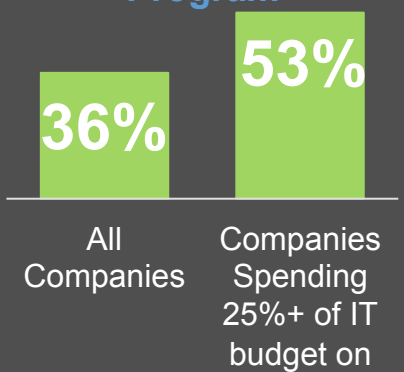
QuickStats
99% of ITDMs feel their organization's software and applications are secure.

ITDMs in Cybersecurity



36% of organizations currently use bug **bounty** programs including 53% of companies that spend 25% or more of their IT budget on APPSEC.

Currently Have Bug Bounty Program



The disconnect between an organization feeling secure while still releasing software code before proper testing is deployed is startling. These facts prove that further education is needed on an organization's approach to overall vulnerability awareness and response. Data from the survey did show however, that many organizations are investing in the proper security tools to address inherent issues.

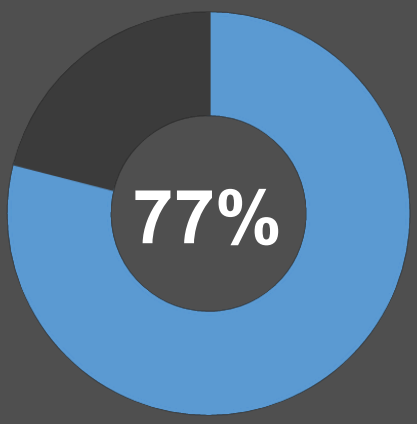
For example: 85% of companies currently have data loss prevention (DLP) in place to prevent end users from sending sensitive information outside of the organization's network; 81% have an application security program in place to find and fix vulnerabilities in their software and protect applications from external threats; 81% have security information and event management (SIEM) to analyze security alerts generated by network hardware and applications; 80% have endpoint detection and response (EDR) to detect and resolve suspicious activity on hosts and endpoints and more than 1 in 3 (36%) have a bug bounty program to reward individuals for identifying bugs in their software.

Although these respondents are clearly taking the proper steps to establishing a strategic approach to security, it's important to keep in mind that a layered approach to application security, specifically, will add enhanced strength and protection to the overall business.

The Truth About Bug Bounty Programs

QuickStats
77% of ITDMs feel as though organizations rely too heavily on bug bounty programs to catch their application security issues.

ITDMs in Cybersecurity



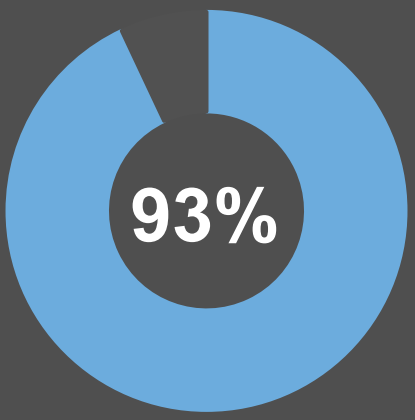
Although 36% of respondents have invested in a bug bounty program, 77% of respondents actually feel as though organizations rely too heavily on these programs to catch their application security issues. Respondents feel this way even though 98% of organizations with a bug bounty program frequently fix a vulnerability through a bug bounty program. In fact, the growing popularity of these programs have even caught the eye of notable technology giants such as Apple, Google and Yelp. Both the payout and "the fix" frequently attract attention and can be effective, but relying on a reactive approach to vulnerability detection is simply not enough.

Companies must understand that bug bounty programs, although helpful, should not be used as a replacement for a strong application security culture and program. Companies must instead embrace a best-of-both worlds proactive approach to efficiently and comprehensively identify and eliminate security threats. There's also the issue of cost. Almost half (44 percent) of respondents have spent $1 million or more on bug bounty programs, which begs the question: Are bug bounty payouts really worth it?" Here's one clue: 79% of cybersecurity ITDMs believe organizations that have application security programs spend less on bug bounty programs than those who don't.

Focusing on Development + Testing Phase

QuickStats
93% of ITDMs believe most flaws found in a bug bounty program could've been prevented by developer training or testing.

ITDMs in Cybersecurity

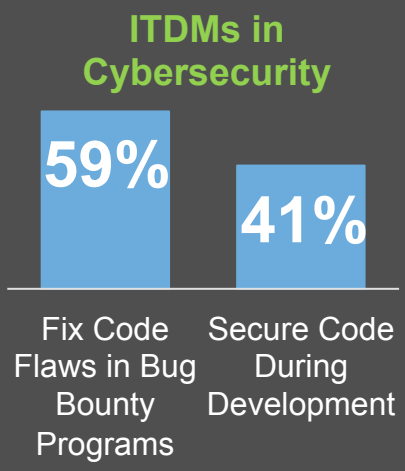


It's vital to devote more resources during the actual software development phase instead of just addressing vulnerabilities once applications are already in use. Simply put, it should not be a matter of one or the other, but instead organizations should consider launching bug bounty programs alongside automated security testing deployment during the development cycle. Consistency is key and something that the respondents who said they allocate resources to automated security testing should reevaluate: 47% don't do this all the time.

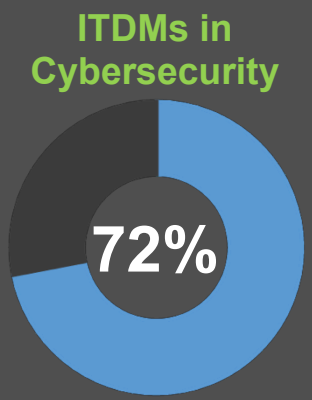
The research finds that 93% of cybersecurity ITDMs believe most flaws uncovered in an organization's bug bounty program could have been prevented by developer training or testing in the development phase. That's why bug bounty programs should only be put in place once backed by a robust application security process. A balanced application security culture is important – and many organizations fall short.

Conclusion: Need for Proactive, Layered Approach

QuickStats
59% of ITDMs think it's more expensive to fix code flaws found in bug bounty programs than to secure code during development.



QuickStats
72% of ITDMs believe their organization focuses more on remediation of vulnerabilities than on proactive or layered security programs.



Consider a Best-of-Both Worlds Approach to Application Security

Organizations should only launch bug bounty programs after they have successfully automated security testing during the development cycle. When bug hunters report issues that could have initially been found through quick static and dynamic testing in the development cycle, it can end up costing an organization more. Indeed, 59% of cybersecurity ITDMs believe it's more expensive to fix code flaws found in bug bounty programs than to secure code during development (41%).

The truth is that cyberattacks at the application layer are common. Even the most mature application security programs will let bugs slip through into production. Resources should be allocated to multiple security precautions. Research finds that 72% of cybersecurity ITDMs believe their organization focuses more on remediation of vulnerabilities than on proactive or layered security programs. This includes 87% of ITDMs whose organization has a bug bounty program.

And keep in mind that for the bug bounty program to work, an organization should have a strong application security program already in place. Otherwise, instead of finding critical flaws in the system, hackers will spend most of their time uncovering common mistakes that could be prevented through secure code development. Find out more about securing your code. Check out why you need APPSEC.

Methodological Notes and Links to Resources

LEARN MORE AT WWW.VERACODE.COM, ON THE VERACODE BLOG, AND ON TWITTER

RESEARCH CONDUCTED BY WAKEFIELD RESEARCH

Wakefield Research (www.wakefieldresearch.com) is a leading, independent provider of quantitative, qualitative, and hybrid market research. Wakefield Research supports the world's most prominent brands and agencies, including 40 of the Fortune 100, in 70 countries.

Methodological Notes:

The Veracode Bug Bounty Survey was conducted by Wakefield Research (www.wakefieldresearch.com) among 500 U.S. IT decision makers working in cybersecurity, between August 23rd and August 31st, 2016, using an email invitation and an online survey. Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 4.4 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.