When it comes to vulnerabilities, organizations face a problem of scale. Even as the vulnerability discovery and management market grows—with a modest gain of about 9.4 percent per year since 2012— the amount of money to test for new and existing vulnerabilities is hardly skyrocketing. Meanwhile, Web-based malware attacks more than doubled in the second half of 2013, the global cost of cybercrime exceeded $400 billion in 2013 and there’s no sign of that pressure letting up.

As the number of applications that enterprises depend on to service customers and satisfy end users continues to increase, so does the number of vulnerabilities in their growing code base. While traditional penetration testing and automated scanning have provided enterprises with some level of success in reducing vulnerabilities, it’s clear that these traditional means of discovery are leaving gaps behind. Clearly, the bad guys are finding vulnerabilities faster than enterprises can.

One look at the data breach statistics bears that out: The number of breached records increased by 233 percent between the first quarter of 2014 compared with the same period in 2013.

Writing secure software is never easy. While developers must worry about securing every vulnerability in their code, malicious hackers have to find only one weakness to exploit. Not only that, but security researchers are hard to find and hire. At the same time, the number and sophistication of malicious hackers probing software for weaknesses continue to grow. So while security teams are limited by the scope of time, money, and sets of eyes looking for vulnerabilities, the bad guys seem to have limitless resources.
the power of

Organizations seeking an efficient way to find vulnerabilities more quickly than the traditional penetration testing route are making inroads through the principle of crowdsourcing. In the bug-finding world, the power of crowdsourcing is harnessed through bug bounties. The idea behind these bounties is simple—to offer cash incentives and public kudos to members of a large but skilled pool of security research freelancers and moonlighters willing to look for them. Rather than paying by the hour for a testing consultant, organizations pay per issue discovered.

Crowdsourced security is not a new idea. Global companies, such as Google, Facebook and PayPal, have been very public about their use of bounty programs to find critical vulnerabilities that may have either gone unfound or cost many hours of consulting time to discover through the traditional route.

These high-powered names are a testament to the power of crowdsourced vulnerability discovery. But programs like theirs are difficult to set up and costly to run in-house. However, it’s a myth that only huge companies with mature bounty programs can get value from crowdsourcing. This report offers the data to prove it.
Over the past year-and-a-half, Bugcrowd broke the mold of the typical bug bounty infrastructure set-up for more precise and efficient vulnerability discovery crowdsourcing. Through trial and error with various enterprise clients, its team devised a new way to divvy up the bug bounty action into bite-sized chunks. The result was formalized into Bugcrowd’s unique Flex Bounty Program, a fixed-cost, two-week crowdsourcing engagement that can be instantly started and still taps into the skills of the research community the way an on-going bounty program does.

Along the way, Bugcrowd has studied the effects of its Flex Bounty Program and now has demonstrable data that shows how—even in small pieces—crowdsourced vulnerability assessments can tip the economic scales from favoring attackers to favoring those who are trying to defend themselves from attacks against previously unknown vulnerabilities.

This is early research, so data collection practices are still being refined. While Bugcrowd has anecdotal stories and insights from 60 Flex Bounty Program engagements, it has collected truly robust data sets for only about one-third of them. The data outlined from this report is based on the company’s nine most complete case studies.
These programs were designed to act as a gateway for an enterprise to initiate an ongoing responsible disclosure or bug bounty program, or to be used to strategically supplement existing security vulnerability testing programs.

Security researchers who sign up at Bugcrowd.com are provided visibility to public bounty programs. Upon agreeing to the Bugcrowd Terms of Service and each bounty program’s testing scope, researchers may then participate in helping discover vulnerabilities for that organization. Private programs are only visible to researchers who meet those program requirements.

**FIXED TIME FRAME:** A typical Flex Bounty Program engagement is two weeks.

**FIXED PRICE:** A Flex Bounty Program customer allocates a predetermined amount into a reward pool, which is then offered to Bugcrowd researchers. The pool is divided and allocated to unique vulnerabilities; the cost to the customer remains fixed, regardless of the number of issues uncovered. Bugcrowd takes a percentage of the reward pool offered as its management fee.

**RAPID DEPLOY:** The sun is always shining somewhere for Bugcrowd’s global pool of security researchers, which means our Flex Bounty Program can be deployed immediately.

**INCREASED CROWD VISIBILITY:** Standard Flex bounties are public to all researchers, which provides the most comprehensive testing coverage. However, some companies have chosen to participate in a closed Flex Bounty Program, which is open only to a select segment of the crowd (e.g., our top 100 security researchers). For even greater control, researcher traffic can be routed through Bugcrowd’s infrastructure as well.

Since 2013, Bugcrowd has conducted 60 fixed-time frame, fixed-scope and fixed-budget testing engagements for customers.
One of the major concerns many organizations have about bug bounties is that while the quantity of results provided may eclipse a traditional test’s volume, the quality of vulnerabilities might not be as strong. Bugcrowd’s data suggests otherwise: The bug bounty incentive structure actually rewards researchers based on the severity of problem detected or creativity of tactics employed. Combined, these incentives prompt the crowd’s competitive urge, resulting in some pretty impressive finds.
Over the course of 60 Flex Bounty Program engagements, Bugcrowd researchers have exposed plenty of hair-raising vulnerabilities while chasing their cash rewards. These vulnerabilities, coupled with the data on valid volume of bugs found, reveal both the breadth and depth in crowdsourced vulnerability discovery. Here are some examples:

**CLOUD PROVIDER EXAMINATION:** In one capture-the-flag bounty competition involving applications tested for a cloud platform developer, a researcher compromised the platform’s Windows host within 12 hours. Another found remote code execution giving full SYSTEM access to approximately 15 percent of the provider’s client’s hosts.

**CMS ZERO-DAY DISCOVERIES:** One Flex Bounty Program conducted for a customer yielded six critical zero-day vulnerabilities on a public content management system (CMS) platform.

**TOTAL IAAS COMPROMISE:** A Flex Bounty Program run for an infrastructure-as-a-service (IaaS) provider attracted a researcher who was able to find and exploit vulnerabilities that achieved a total platform compromise within 25 minutes and a shell on the underlying box within 90 minutes.

WHERE RESEARCHERS RESIDE

**TOP GEOGRAPHIES**

Another myth about bug bounty programs is that a pool of crowdsourced researchers could comprise unqualified workers from less technically mature parts of the world. Again, Bugcrowd’s research suggests otherwise, both in geography and level of expertise:

- **UNITED STATES**
- **INDIA**
- **UNITED KINGDOM**
- **AUSTRALIA**
- **NETHERLANDS**
- **GERMANY**
Each unique vulnerability is rewarded at the end of the Flex Bounty Program. The top three most severe and creative issues are selected and rewarded a “placed reward.” The remaining bugs are rewarded an “unplaced reward.” If there are more bugs found than there is money in the reward pool, the unplaced reward tier is diluted to ensure that all researchers in that tier are compensated. Conversely, if the pool isn’t fully allocated, the leftovers are carried forward to the next time the company runs a Flex Bounty Program (which is where a direct cost saving for better code security practices starts to kick in).

**REWARD POOL BREAKDOWN (BASED ON $10,000 REWARD POOL):**

- **1ST**: $2,500
- **2ND**: $1,500
- **3RD**: $500

**UNPLACED**: $250 ea. or the remainder of the pool ÷ by the number of remaining bugs, whichever is lower.

**AVERAGE TOTAL PRICE:**

- **$11,614**: Average prize pool per Flex Bounty Program
- **$12,000-$20,000**: Typical 2-week penetration test consulting engagement (estimate)
Bugcrowd sponsored a Flex Program to test four different mobile applications on four different platforms. Bugs found through this Flex Program spanned across all categories of the OWASP Top 10. Some of the issues discovered included:

**Moderate Risk**
- Insufficient transport layer protection
- Poor authorization and authentication
- Broken cryptography
- Client side injection
- Security decisions via untrusted inputs
- Lack of binary protections

**High Risk**
- Unintended data leakage
- Insecure data storage

**Results**
- 3 weeks testing window
- $12,500 pool
- 318 researchers
- 238 total submissions
- 75 valid submissions
In one instance, Bugcrowd helped a mobile application development startup test its application prior to launch via a Flex Bounty Program. Within 90 minutes of the bounty’s start, security researchers were able to compromise the application infrastructure through some of the following vulnerabilities:

- The application had a SQLi in the OAuth authentication process.
- DB hashes were pulled out of the database, which did not have proper access control.
- DB hashes were then cracked. The admin user was root:root.
- The admin user was used to escalate to the system, at which point the tester contacted Bugcrowd via the escalation process.

Many of the findings of this test involved identification of privacy settings—problems that couldn’t be easily identified by automated scanning techniques.

Two weeks may be fast for some, but not quite enough for one of Bugcrowd’s customers. Due to very short change windows in its IT infrastructure, the customer needed vulnerability test results within 24 hours. The efficiency and flexibility of rapid deployment offered by the Flex Bounty Program made that turnaround possible. The Flex Program for that customer managed to fit 80 man-hours of work into 24 hours of actual time.
Price points are only part of the economic picture—the true measure of returns offered by two-week bounty engagements is their efficiency. Bug bounties enable enterprises to put more security researchers on the hunt for vulnerabilities more quickly than traditional penetration testing engagements.

Bugcrowd’s early work with the Flex Bounty Program has shown that it is possible to take advantage of crowdsourced security without requiring the infrastructure of a fully mature bounty program.

Similarly, if you already have a program in place but need to quickly spin up resources, Bugcrowd’s Flex Bounty Program offer an option beyond traditional security consulting. A multinational and diverse pool of researchers offers far more availability than a homogenized team from a typical consulting firm, no matter how big the company. This makes for a faster start and finish to testing.
Bugcrowd, the innovator in crowdsourced security testing for the enterprise, was founded in 2012 by a team of security and software development experts who saw the opportunity to level the playing field in cybersecurity. Bugcrowd’s revolutionary approach to cybersecurity combines a proprietary vulnerability reporting platform with the largest community of security researchers on the planet.

Bugcrowd offers Responsible Disclosure and Bug Bounty programs in addition to the new Flex Bounty Program (a limited time, fixed-cost introduction to the benefits of crowdsourcing). Bugcrowd has run over 80 bounties with over 9,500 researchers who have submitted over 13,700 bug reports to-date.

GET IN TOUCH WITH BUGCROWD:
- To learn more about our Responsible Disclosure, Bug Bounty and Flex Bounty programs, click here
- For all our news, check out the Bugcrowd blog
- For journalists with questions, e-mail press@bugcrowd.com

© 2014 Bugcrowd. All rights reserved. Bugcrowd is a trademark of Bugcrowd.