Hiring Hackers

Want to strengthen your digital security? Pay someone to break into your software—and your systems

LAST MAY, UNITED AIRLINES, still struggling to integrate its computer system with Continental's following the merger of the two companies, issued an open call to hackers. The challenge: to locate and report security holes on its website, with airline miles as an incentive for successful finds. Uncovering a scripting flaw could earn 50,000 miles, while a vulnerability that allowed denial-of-service attacks could score 250,000 miles. Within two months, the Chicago-based carrier had shelled out 1.8 million miles for several bugs, including two so-called remote code execution flaws that could have let a hacker take over United's system.

United's experience reflects a sobering truth: No matter how many hours your digital team sweats it out in front of a computer, they're never going to find and patch every vulnerability. And even if you pay an outside firm to do the job, it almost certainly won't find everything either. But a boundless, global army of hackers who are paid only when they unearth security bugs? Now you're talking.

Once the purview of tech giants like Facebook and Google, this model has gone mainstream. Today, hundreds of companies host so-called bug-bounty programs spanning apps, software, and company networks. Some companies have invitation-only programs. Many post program guidelines on their websites, including a schedule of payouts based on the seriousness of a flaw.

So how do you throw open your arms to ethical hackers without wasting your time or—far worse—exposing something critical that someone can exploit? A few pros share their insights.
—KATE ROCKWOOD

Start With Self-Scrutiny

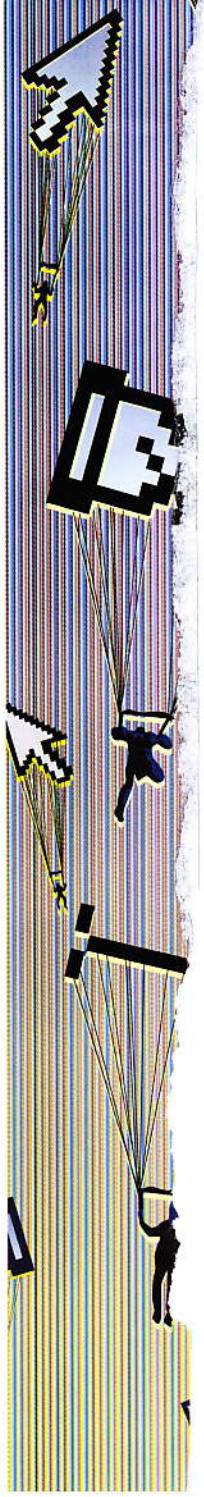
Eager as you might be to get going with a public program, your first step should be internal testing. "If you don't have your house in order or your security is terrible, researchers could swarm you and it'll be harder to sift through what's legitimate," says Manoj Kasichainula, head of security at San Francisco–based Asana, which makes team productivity software. And if you're flooded with duplicate reports, you'll either spend a lot of extra money or, if your program is first come, first served, annoy a lot of hackers.

Don't Fret a Small Budget

You don't have to flash a big payout to attract talented hackers. Sure, Google has shelled out more than $4 million over the past five years. But companies from Apple to Airbnb run programs with no monetary reward at all, instead shouting appreciation from the digital rooftop. "I think linking to people is rewarding, so I'll always ask if they want to include their LinkedIn or Twitter URL," says Grant Stavely, a senior security engineer at Evernote, a Redwood City, California, maker of productivity apps. To stretch the prize money you have, set parameters around what you're willing to pay for. When Helsinki-based F-Secure launched a bounty program in November, it included most consumer and corporate products but not bugs on the company's main webpages. "Our website is like a promotional face," says security adviser Sean Sullivan. "It's far more important that our products and customers are secure." Payouts don't have to be huge, either. According to security specialist Bugcrowd, the average payout for the more than 300 programs it helps manage is $250 or so.

Think Through the Workflow

When hackers spot a bug, where do those emails go? Who vets the reports to determine whether the bug is legit? "You need people



BUG BOUNTY BALLERS

Companies with a lot at stake in their data security have ponied up some major prizes

$15,000
Initially heckled for awarding company swag as bounties (a.k.a. T-shirtgate), Yahoo gave Ibrahim Raafat of Egypt its top bounty in 2014 for spotting a bug in Flickr's photo-printing app that left its server and database vulnerable.

$33,500
in 2013, Facebook paid Brazil's Reginaldo Silva one of its largest bounties for exposing a bug that could let a user hijack someone else's computer.

SPREAD FROM LEFT: DAVID DE STEFANO/GETTY; JOSEPH CLARK/GETTY

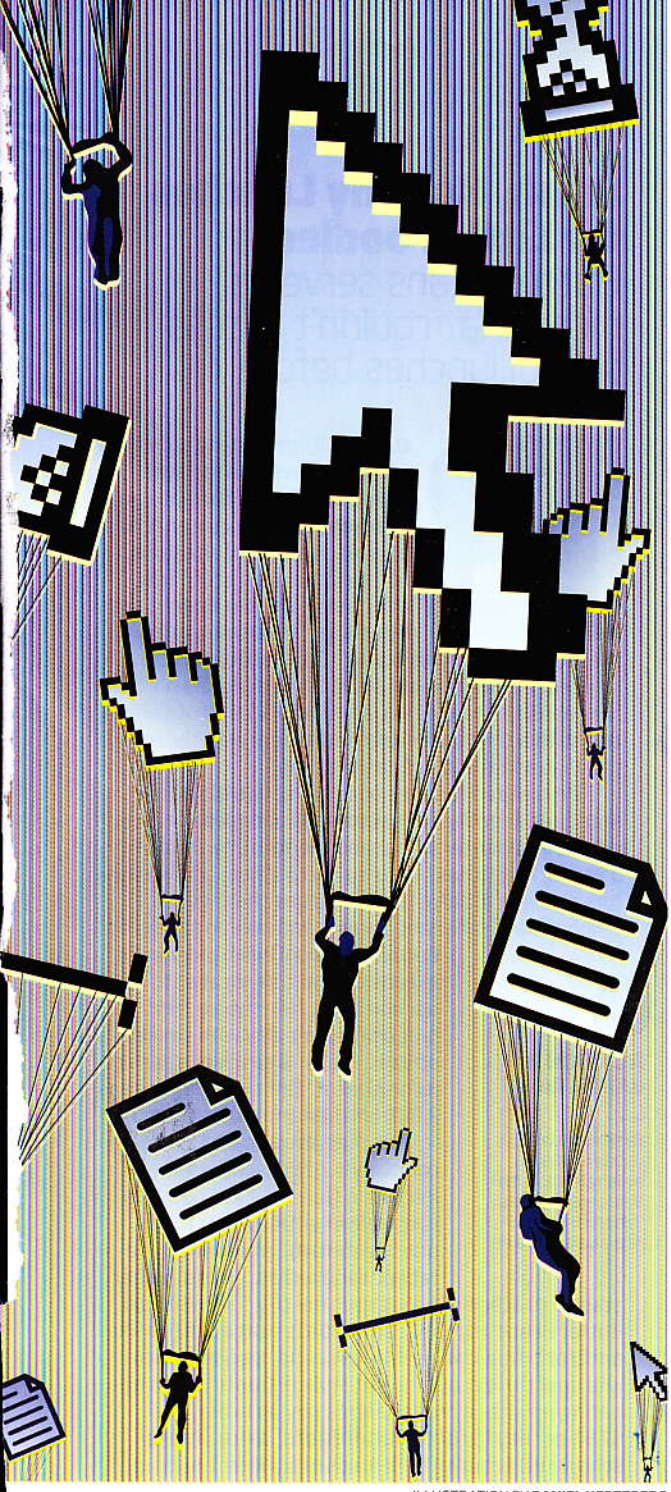


ILLUSTRATION BY **DANIEL HERTZBERG**

with good judgment on the frontlines, because if you have someone who misinterprets the reports, everybody gets really frustrated really quickly," says Kasichainula. There's no way to predict the pace of submissions, but even when your team is inundated, promptly acknowledge bug reports when you get them. If you seem inattentive to user safety, you risk a researcher's disclosing the bug publicly while you're still sorting out how to patch it.

↓

Don't Go It Alone If You Don't Want To

If the idea of coordinating an international payment to a hacker feels somewhat fraught, fear not. Startups including HackerOne and Bugcrowd can help get your program up and running and even manage payouts. "There's a learning curve to running these programs, and when you're just starting out you might be busy enough dealing with the development schedule," cautions Sullivan. But calling in the pros doesn't mean outsourcing the whole endeavor. You might be better off scrutinizing vulnerability reports in-house. Leaving out the middleman when you're working on your own code tends to mean fewer mistakes and faster fixes.

PSSST! THIS BOUNTY IS INVITE ONLY

Before you bring on all comers, you might want to take a trial run

—

For every bug-bounty program that has a detailed webpage for all to read, there's at least one private program that almost no one knows about. "It's not one-size-fits-all," says Alex Rice, CTO and co-founder of HackerOne and former head of product security at Facebook. HackerOne—which by late 2015 had coordinated some 2,000 hackers who made over 15,000 bug fixes for more than $5 million in prize money—runs 100 public bug-bounty programs and more than 400 private ones. So how do you know if private is the way to go?

Though recruiting lots of eyeballs can mean more varied and creative hacking, if you're taking your first dip in the bug-bounty pond, Rice recommends starting with an invitation-only pilot, which involves asking a limited number of researchers to hack their hearts out in search of specific vulnerabilities. "If you invite five researchers and they find dozens of bugs in the first 24 hours, you probably don't want to go public," says Rice. "But when you reach a point at which the tempo has slowed and you open it to the whole internet, you'll have so much confidence."

$100,000

Microsoft awarded its first-ever six-figure bounty in 2013 to U.K.-based James Forshaw for reporting a bug that worked around security protections in Windows 8.1.

$150,000

When New Jersey-raised George Hotz hacked into Google's Chrome operating system in 2014, Google gave him its highest individual bounty to date—and a job.

One million miles

Last July, United Airlines gave Florida researcher Jordan Wiens not moolah but megamiles for finding a bug that could help someone take over a remote computer.