hackerone

THE HACKER POWERED SECURITY REPORT 2019

The study on the hacker-powered security ecosystem

@try_to_hack: first hacker to achieve $1M in bounties

Executive Summary

Hacking is here for good, for the good of all of us. Half a million hackers have willingly signed up with HackerOne to help solve one of the greatest challenges our society faces today. We cannot prevent data breaches, reduce cyber crime, protect privacy or restore trust in society without pooling our defenses and asking for external help.

The positive power of the hacker community far exceeds the risks and the might of adversaries. To date, HackerOne has helped find and fix over 120,000 vulnerabilities for 1,400 client organizations, earning hackers more than $62 million in awards—nearly half of that in the past year alone. A quarter of valid vulnerabilities found are classified as being of high or critical severity. When a new bug bounty program is launched, in 77% of the cases, hackers find the first valid vulnerability in the first 24 hours. That is how fast security can improve when hackers are invited to contribute.

Yet the work is not done. It has barely begun. Each day we must fear the discovery of yet another giant data breach. The number and the magnitude of the breaches keep growing. At risk are financial institutions, healthcare organizations, e-commerce companies, big box stores, media companies and practically anyone relying on technology.

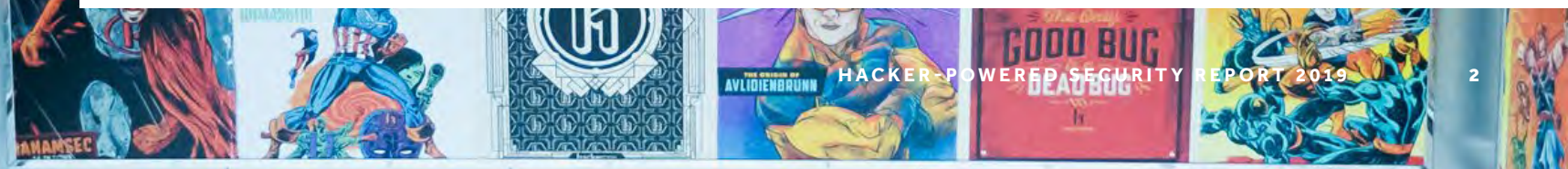
But some of the most recent breaches have one thing in common: they were detected, discovered and reported by good hackers.

Hackers are no longer anonymous guns-for-hire. They are being embraced by everyone from the insurance industry to government agencies. Hacker-powered security is today a given part of a mature and proactive security program.

It's not hard to see why. Businesses process more sensitive data and more personal information than ever before. Software development lifecycles are increasingly continuous. As companies work overtime to push code, criminals work overtime to find ways to break in. It feels impossible to scale security with product development. Innovation is outpacing traditional security measures.

Working with hackers allows you to provide security at the speed of innovation.

The number of hacker-powered security programs is rapidly growing all over the world. Latin America saw record growth of 41% over the previous year. The federal government sector grew an impressive 214%.



The professionalism and positive impact of hacking is also growing at an impressive clip. In the past year, HackerOne paid out 511 individual bounties of $10,000 for issues of critical severity, a four-fold increase over the year before. The average bounty for a critical vulnerability increased nearly 50% in just one year to $3,384. And yet that is an incredibly low price for a company to pay for the ability to block a weakness that otherwise could be the cause of a data breach.

Hacker rewards are going up both on a unit level and in the aggregate. United States, India, Russia, Canada and Germany are the top earning countries for hackers. Over 50 hackers earned over $100,000 in the past year. A full half-dozen have surpassed $1 million in lifetime rewards.

Society is embracing the positive power of hacking. Lawmakers are introducing legislation to drive hacker-powered security. Government agencies are launching bug bounty and vulnerability disclosure programs. Noteworthy customers include the European Commission, U.K.'s National Cyber Security Centre, Singapore's Ministry of Defense, and, for several years, the U.S. Department of Defense, including the Army, the Air Force and the Marine Corps.

Hacker-powered security is on the rise in risk-averse and highly regulated industries such as financial services, banking, insurance, healthcare and education. With HackerOne's new pentesting and compliance offerings, such companies can fulfill security obligations in a way that's less costly yet more productive. Today, six of the top ten financial services organizations in North America, and companies like Goldman Sachs, PayPal, and Lending Club, are working with HackerOne.

We explore these trends and more in this report. It is the industry's most comprehensive report on security delivered by hackers. The data comes from HackerOne's community of hackers and the database of vulnerabilities reported and resolved. Unless otherwise stated, numbers represent the 12 months from May 2018 through April 2019.

The only way to achieve digital security is to acknowledge that all software contains vulnerabilities and an external unbiased eye is best at spotting them. We will be discussing these vital topics at the Security@ conference in San Francisco on October 15th, 2019.

INTRODUCTION

450K+

TOTAL REGISTERED HACKERS

120K+

TOTAL VALID VULNERABILITIES SUBMITTED

$62M+

TOTAL BOUNTIES PAID

**As of August 2019*

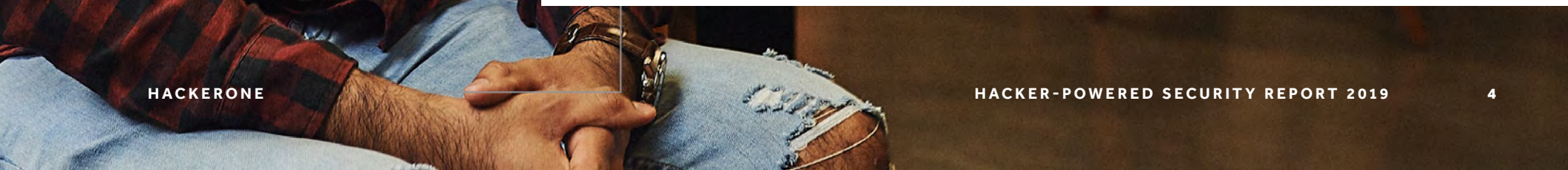
Every five minutes, a hacker reports a vulnerability. Every 60 seconds, a hacker partners with an organization on HackerOne. That's more than 1,000 interactions per day.

The more than 450,000 hackers registered on HackerOne find vulnerabilities missed by traditional detection methods. These trusted hackers—90% of whom are under the age of 35—play a critical role in securing organizations large and small.

Security vulnerabilities are a fact of life. For this reason, technology unicorns, e-commerce conglomerates, governments around the world, and hospitality giants are competing to attract hackers who have one key advantage over traditional methods: they can think like an attacker.

The stories of these hackers are inspirational. They're an invaluable extension of the most trusted security teams, on a mission to find what others may have missed or could not see.

Hackers are the solution to the world's cybersecurity challenges. By investing in people, not just software, we will see the greatest outcome. It is our mission to empower the world to build a safer Internet. This report is a glimpse into how hackers and organizations are doing just that.




EXIT

CONTENTS

IMPORTANT TERMS

Hacker: One who enjoys the intellectual challenge of creatively overcoming limitations.

Hacker-Powered Security: Any goal-oriented hacking technique that utilizes the external hacker community to find unknown security vulnerabilities and reduce cyber risk. Common examples include private bug bounty programs, public bug bounty programs, time-bound bug bounty programs, hacker-powered penetration testing for compliance, and vulnerability disclosure policies. With hacker-powered security testing, organizations can identify high-value bugs faster with help from the results-driven ethical hacker community.

Hacker-Powered Penetration Test: A limited access program where select hackers apply a structured testing methodology and are rewarded for completing security checks.

Hacktivity: Hacker activity published on the HackerOne platform.

Public Bug Bounty Program: An open program any hacker can participate in for a chance at a bounty reward.

Private Bug Bounty Program: A limited access program that select hackers are invited to participate in for a chance at a bounty reward.

Time-Bound Bug Bounty Challenge: A limited access program with a predetermined time frame where select hackers have a chance at earning a bounty award.

Vulnerability: Weakness of software, hardware or online service that can be exploited.

Vulnerability Disclosure Policy (VDP): An organization's formalized method for receiving vulnerability submissions from the outside world, sometimes referred to as "Responsible Disclosure." This often takes the form of a "security@" email address. The practice is outlined in the Department of Justice (DoJ) Framework for a Vulnerability Disclosure Program for Online Systems and defined in ISO standard 29147.

Key Findings

01 **The average bounty paid for critical vulnerabilities increased to $3,384** in the past year. That's a 48% increase over last year's average of $2,281 and a 71% increase over the 2016 average of $1,977. Bounty values for less severe vulnerabilities are also rising, with the average platform-wide bounty increasing 65% from last year.

02 **Federal Government had the strongest year-over-year industry growth at 214%,** and last year saw the first launch of programs at the municipal level. This strong growth was followed by Automotive (113%), Telecommunications (91%), Consumer Goods (64%), and Cryptocurrency & Blockchain (64%). For the fifth year in a row, every industry increased their participation in the hacker-powered security market by adding net new programs.

03 **The majority of bug bounty programs remain private** at 79% with little change from years prior. Public programs engage 6 times as many hackers from the Technology sector, with Internet & Online Services at 32% and Computer Software at 22%, followed by Cryptocurrency & Blockchain and Media & Entertainment tied at 9% each. 50 total programs advanced from private to public in the last year.

04 **Today six out of 10 of the leading financial services organizations in North America are running hacker-powered security programs on HackerOne.** Financial services organizations running hacker-powered security programs increased 41% this year.

05 **Six hackers surpassed $1 million in lifetime earnings, seven more hit $500,000 in lifetime earnings, and more than 50 earned $100,000 or more in the past year alone.** Skilled and dedicated hackers have the potential to build a career and make a competitive living with the opportunities offered by hacker-powered security.

06 **Globalization of hacker-powered security continues to increase.** Several new countries entered the top 10 highest paying, hackers living in 19 countries earned more than $100,000 in total last year, and more organizations in more countries are hosting live hacking events. We've paid hackers from 112 countries, that's 57% of all the countries in the world. We've had hackers submit reports from 163 countries: that's 84% of all the countries in the world.

07 **Hacker-powered pentests on the rise** as organizations are using hackers to bring realistic simulations of real-world attacks to security testing. In a recent report, one organization detailed how hacker-powered pentests helped them eliminate $156,784 in total costs and save an additional $384,793 over three years by reducing internal security and application development efforts.

Hacker-Powered Adoption and Bounties by Geography

What was once a phenomenon confined to North America has now become a global trend. The number of hacker-powered security programs has grown by at least 30% in each region, with Latin America leading the pack again with year-over-year growth of more than 41%, followed by North America (34%), EMEA (32%), and APAC (30%).

Organizations located in the U.S. paid 83% of all bounties to hackers around the globe, the same share as last year. Canada-based organizations remain in the second spot, while those in the U.K. are in third place, both maintaining their positions from last year. Israel and Belgium entered the top 10 highest paying countries for the first time.

Hackers are also continuing to earn more money no matter where they reside. In just the past year, more than 50 individual hackers earned $100,000 or more. And in the past few months, six hackers have surpassed $1 million in total bounties earned while another seven hackers exceeded $500,000 in total earnings. These top earners are just as global as the organizations seeking their help, hailing from Argentina, Australia, Belgium, Canada, Hong Kong, Sweden, and the U.S.

Hackers in the U.S. earned 19% of all bounties last year, with India (10%), Russia (6%), Canada (5%), and Germany (4%) rounding out the top five highest-earning countries. Hackers in Canada saw the most earnings growth with 148% more bounties earned versus 2017.

Prolific hackers reside in Egypt, Argentina, Sweden, and Thailand, each of which had hackers earning a combined 200% or more than in the previous year. Thailand hackers earned 467% more than they did in 2017.

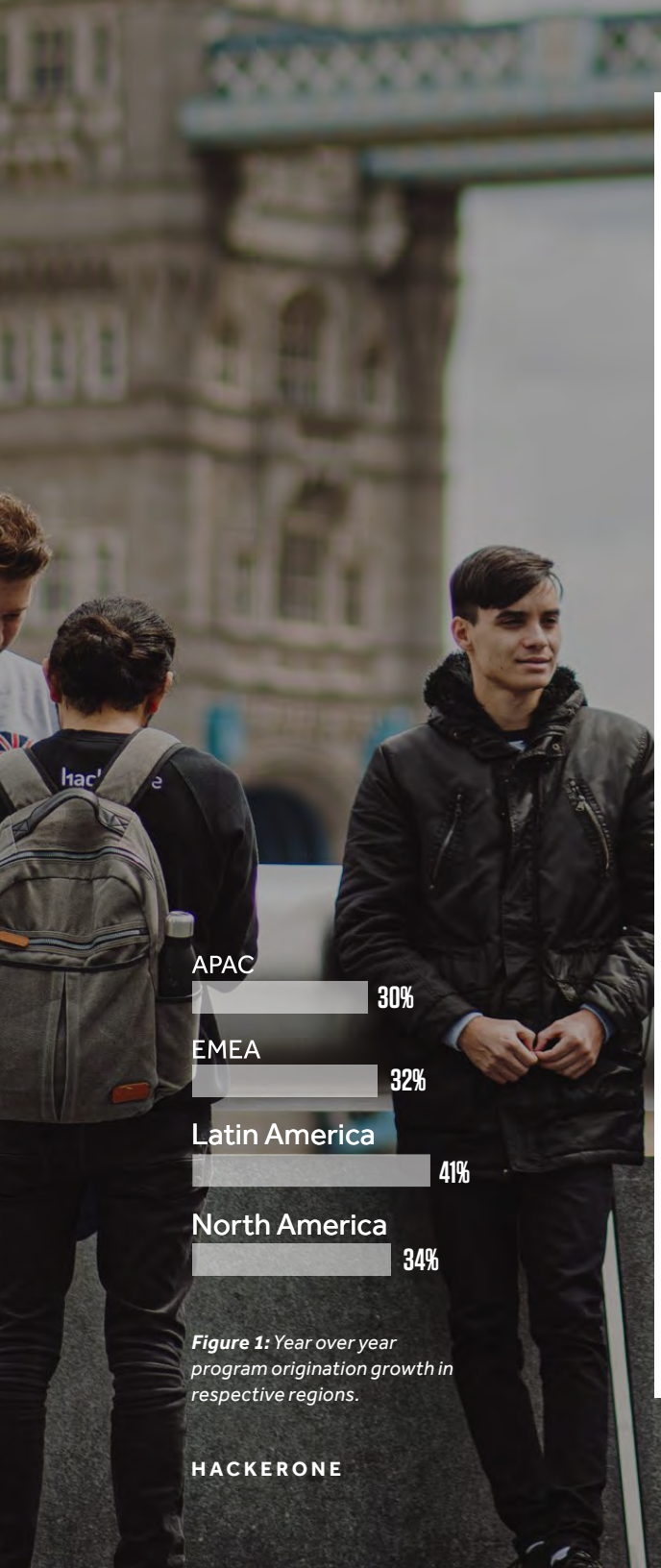


Figure 1: *Year over year program origination growth in respective regions.*

BOUNTIES BY GEOGRAPHY

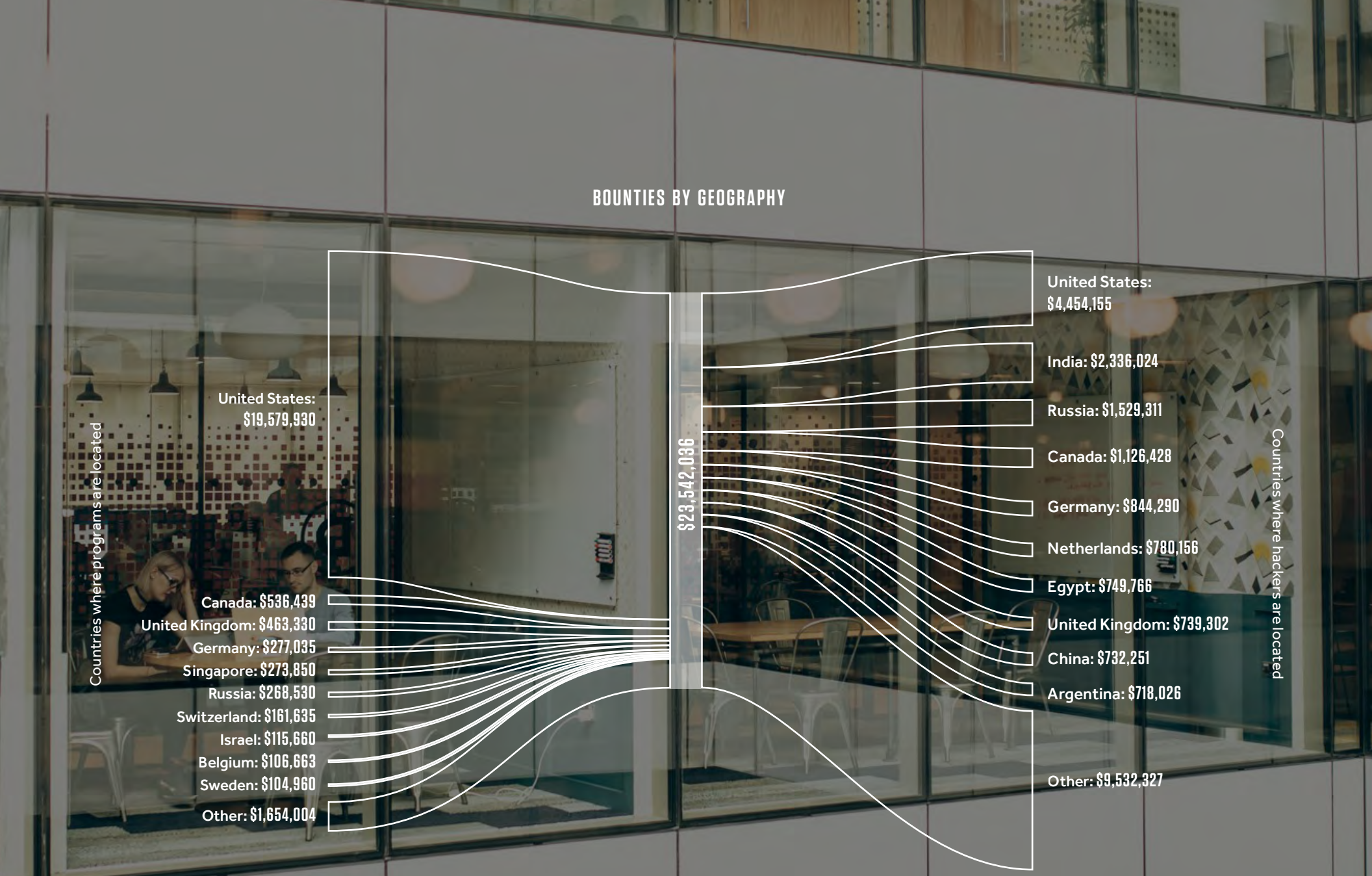


Figure 2: *Visualization of the bounty flow by geography showing on the left where the companies paying bounties are located and on the right where hackers receiving bounties are located.*

Building a Global Community for a More Secure Tomorrow

With more than 1,400 organizations from 59 countries using HackerOne, there are huge opportunities for HackerOne's community of 450,000 hackers. These talented and creative individuals, hailing from more than 160+ countries, use their diverse skills, perspectives, and approaches to help make the Internet a safer place.

The globalization of the Internet has driven the growth of the hacker community, which has further driven the growth of hacker-powered security itself. Smart, creative hackers can access lucrative and challenging cybersecurity opportunities from anywhere in the world—all they need is an Internet connection. Similarly, when smart organizations want to utilize the best hacker talent, they look beyond borders.

Countries as diverse as Iceland, Ghana, Slovakia, Aruba, and Ecuador have hackers with as much determination, skill, and success as those from hacker homes you might expect, like India, the United States, Russia, Pakistan, and the United Kingdom. Likewise, organizations in Argentina and Austria, Belize and Belgium, and Cyprus and Chile—as well as Australia, Brazil, China, and many more—are all enhancing their cybersecurity.

The globalization of hacker-powered security has been spurred by regulations like the European Union's (EU) installation of the General Data Protection Regulation (GDPR) and the Centre for European Policy Studies (CEPS) guidelines for vulnerability disclosure across the EU.

But individual governments are also contributing to the globalization of hacker-powered security by leveraging the vast and varied community of international hacker talent. The U.S. Department of Defense has detected more than 10,000 security vulnerabilities with HackerOne. The European Commission, UK's National Cyber Security Centre, Singapore's Ministry of Defense and Government Technology Agency are also finding success with hackers by identifying vulnerabilities in their public-facing systems.

Looking specifically at the size of organization, there was an 82% increase in enterprises launching programs compared to years prior. Notable launches of hacker-powered programs across industries in the past year include Priceline, Capital One, Hyatt, Backblaze, TomTom, Trustpilot, Credit Karma, Postmates, EU FOSSA, Magento, Ford, Grammarly, FanDuel, Flickr, Casper, Alibaba, PayPal, and IBM.

Though this community thrives on the internet, HackerOne also brings hackers together through live hacking events around the world. This gives customers the opportunity to build relationships with the hacker community in person. These events increase hacker engagement on mature programs, support customer recruiting efforts, and result in thousands of resolved security vulnerabilities for the likes of Uber, Dropbox, GitHub, Shopify, Verizon Media, U.S. Air Force and the U.S. Marine Corps. With highly skilled hackers collaborating on the same attack surface, critical vulnerabilities that could have existed for years are instead uncovered in days. Recent live hacking events have taken place in San Francisco, London, Amsterdam, Singapore, Las Vegas, and other cities around the world.

The fight for Internet security is global. From its San Francisco headquarters to existing offices in London, New York City, Washington DC, Singapore, France, and the Netherlands, HackerOne aims to empower the hacker community and organizations globally to reduce their security risk through collaboration.

To learn more about live hacking events, visit hackerone.com/live-hacking.

WHERE HACKERS ARE LOCATED IN THE WORLD

Figure 3: *Geographic representation of where hackers are located in the world. Remaining countries are each ≤5% of the HackerOne population.*

Programs

The bug bounty program is the most advanced form of hacker-powered security. It provides continuous security testing and vulnerability reports from the hacker community.

Bug bounty programs can be either public or private. Public bug bounty programs, like Starbucks, GitHub, and Airbnb, are open to everyone, while private programs require individual hackers to be invited or accepted through an application process to participate. Public programs are open to the widest range of hacker diversity and therefore produce superior results. On average, **public programs engaged six times the number of hackers reporting valid vulnerabilities.** That's nearly doubled from last year.

Similar to past years, private programs make up 79% of all bug bounty programs on HackerOne, whereas public programs make up the remaining 21%.

By starting with a private program, security teams can then work with a smaller group of hackers to identify unknown and easily found vulnerabilities as they optimize internal security processes. This allows them to become comfortable with the volume and types of vulnerability reports they might expect to receive before advancing to a public bug bounty program. In the past year, 50 programs advanced from private to public.

Most of the public bug bounty programs are run by technology companies, with Internet & Online Services accounting for 32% of all public programs, followed by Computer Software at 22%, and Cryptocurrency & Blockchain and Media & Entertainment tied at 9% each. Private programs are similarly distributed, led by Internet & Online Services at 27%, Computer Software at 21%, Financial Services & Insurance at 8%, and Media & Entertainment at 7%, and Computer Hardware and Retail & E-commerce tied at 5%.

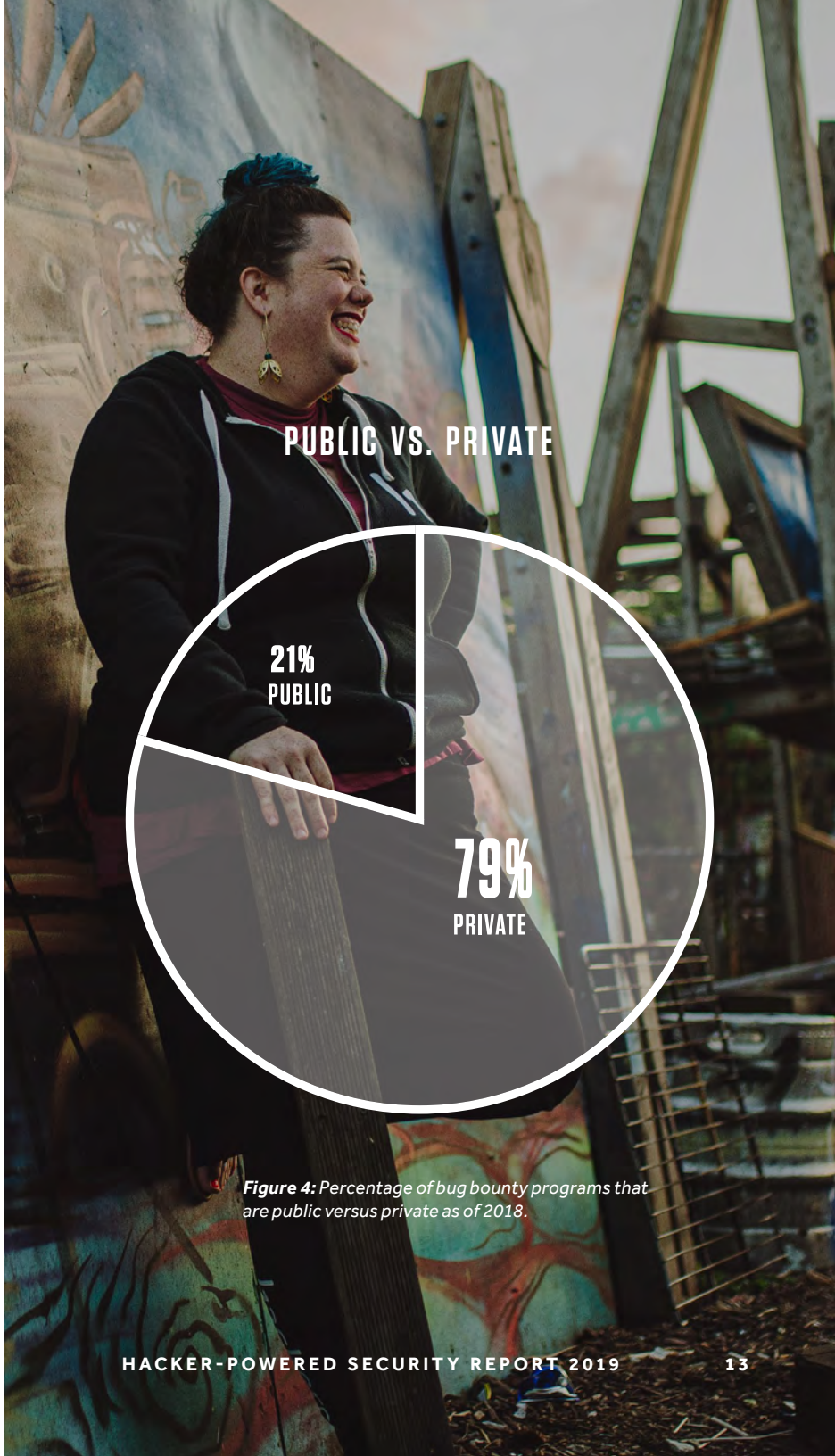
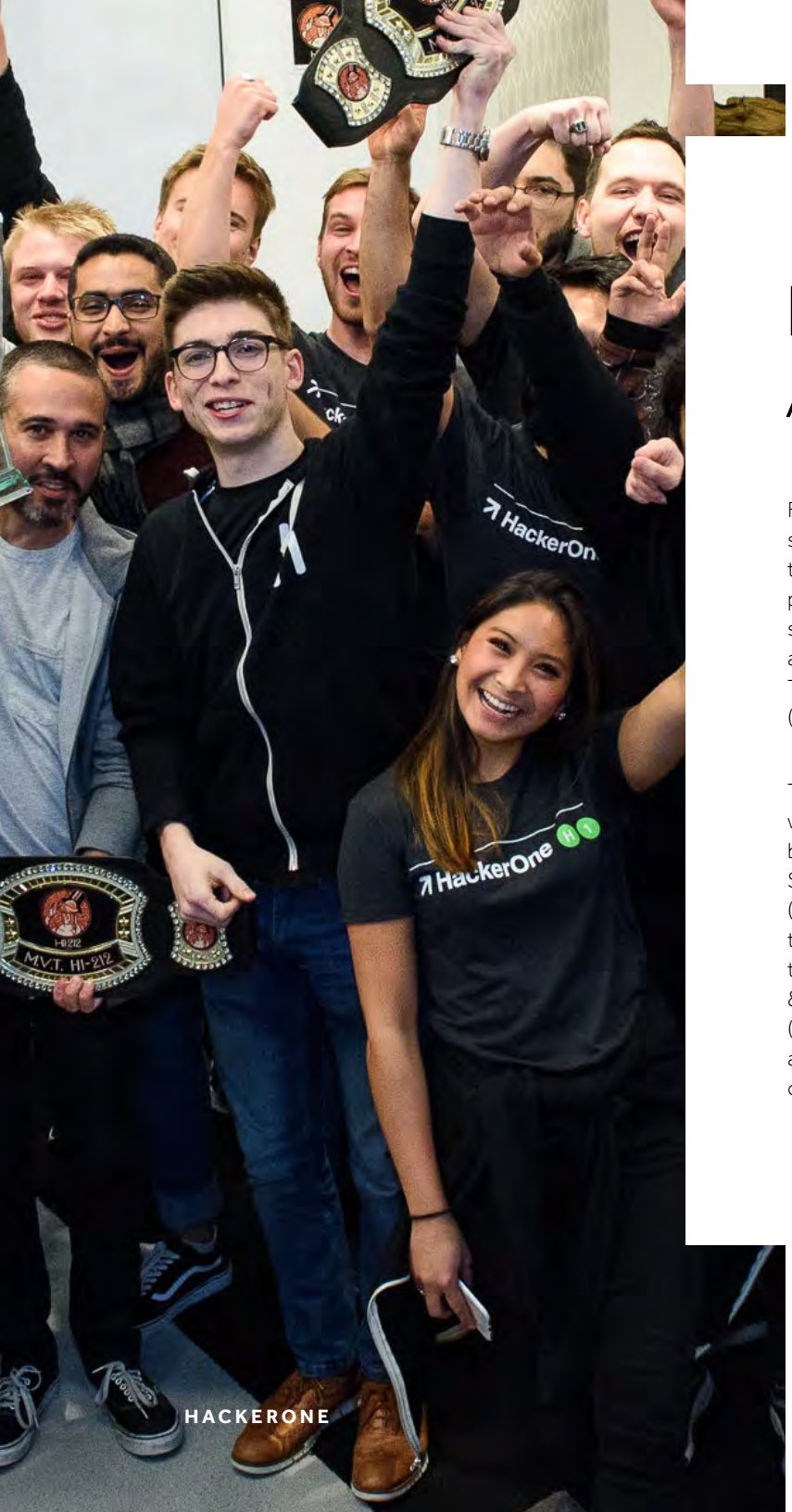


Figure 4: *Percentage of bug bounty programs that are public versus private as of 2018.*



Bug Bounty Program Adoption by Industry

For the fifth year in a row, every industry segment increased their participation in the bug bounty market by adding net new programs. Federal Government had the strongest year-over-year industry growth at 214%, followed by Automotive (113%), Telecommunications (91%), Consumer Goods (64%), and Cryptocurrency & Blockchain (64%).

Technology companies still lead the pack with a combined 60% of all active bug bounty programs, with Internet & Online Services (28%) and Computer Software (21%) making up nearly half of the overall total. However, the rapid growth in non-technology industries puts Financial Services & Insurance (8%), Media & Entertainment (7%), and Cryptocurrency & Blockchain (5%) as the remainder of the top five industries in overall bug bounty program participation.

Financial Services organizations, which are responsible for some of the most sensitive personal information, realized a 41% increase this year. Today six out of 10 of the top financial services organizations in North America are running hacker-powered security programs with HackerOne to identify unknown security vulnerabilities.

In Local Government, we are seeing a rise in security investments at the state and local level for the first time. Recent ransomware attacks have crippled operations across Texas, in Baltimore and Atlanta, and even rural areas, like Garfield County, Utah, Lake City, Florida, and La Porte County, Indiana, demonstrating that organizations of all sizes must enhance security measures.

INDUSTRY BUG BOUNTY PROGRAMS

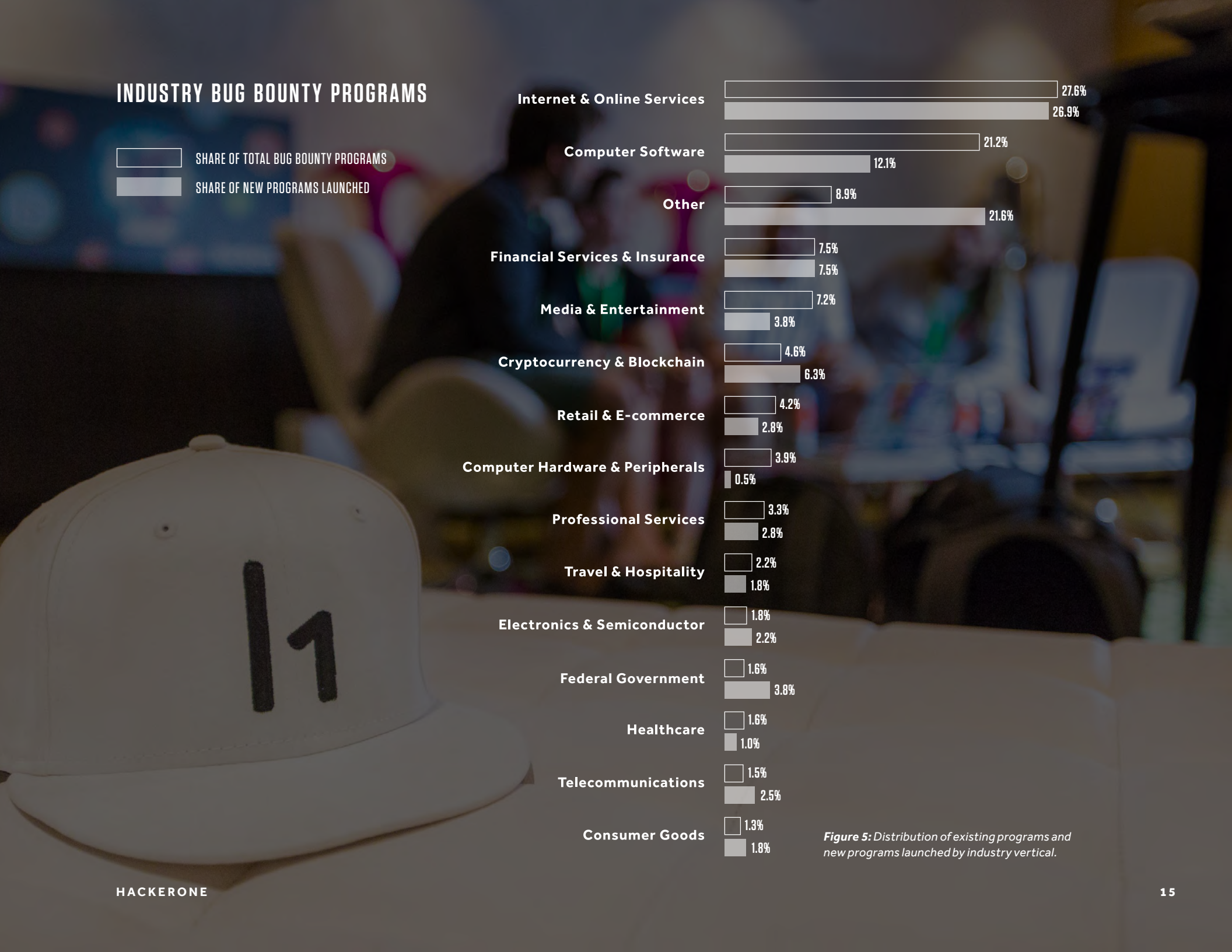


Figure 5: *Distribution of existing programs and new programs launched by industry vertical.*

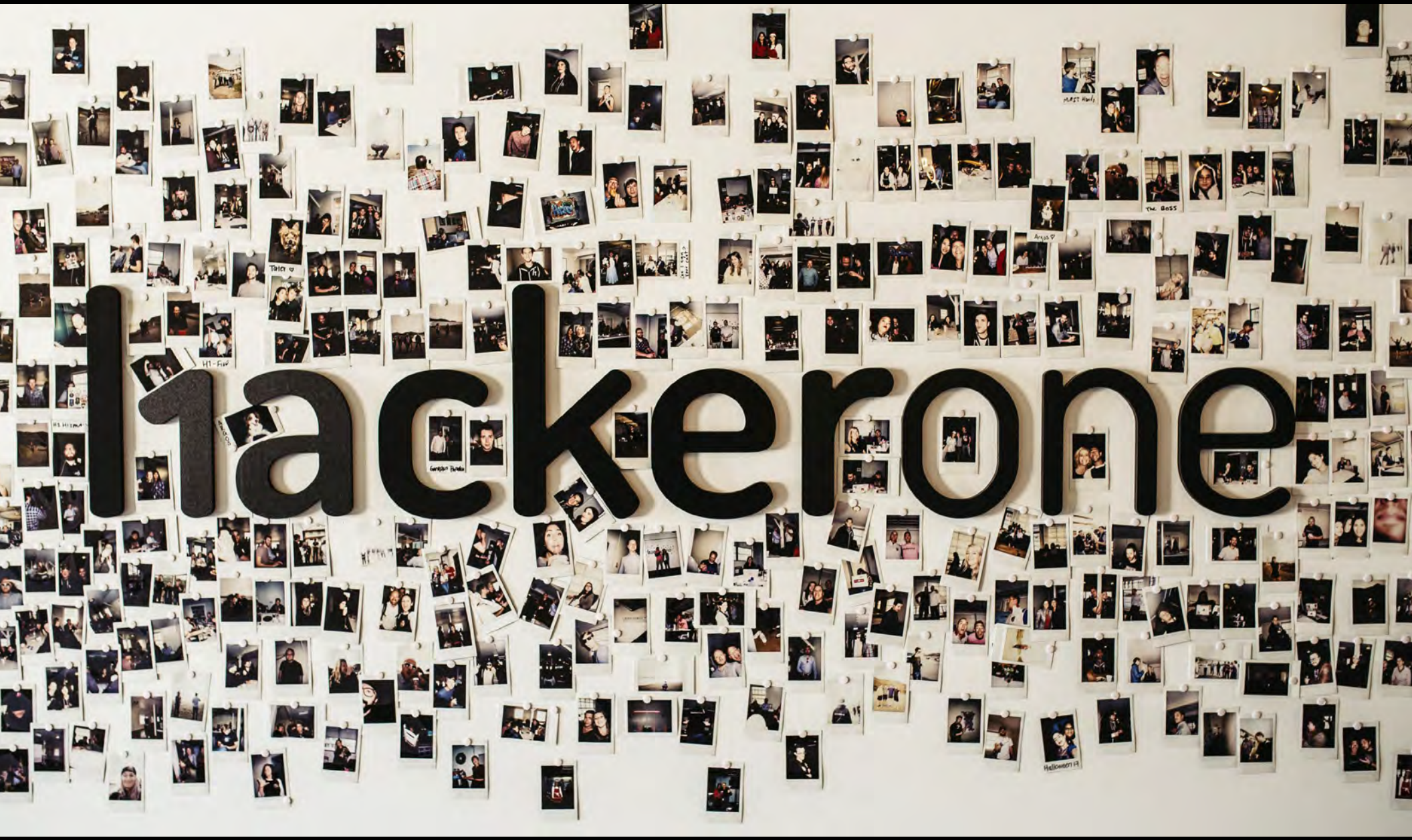
Vulnerabilities by Industry

As of May 2019, more than 123,000 unique valid vulnerabilities have been resolved on HackerOne, with 25% of those—30,541—resolved in the past year alone. Each one of these vulnerabilities represents a real world-risk that was safely mitigated. Without hacker-powered security, many of these critical vulnerabilities would still be at large.

Of the top vulnerability types reported on HackerOne in the past year, cross-site scripting (XSS, CWE-79) remains the most common vulnerability type overall and across nearly all industries. This has been the case for several years, but more industries are starting to see Information Disclosure (CWE-200) surpass XSS as the most common vulnerability type. These include Cryptocurrency, Government, Professional Services, and Retail & E-commerce.

Overall, XSS accounted for 16,290 vulnerability reports submitted, 40% more than the second most common vulnerability type, Information Disclosure, which accounted for 11,634 reports. Several vulnerability types fell out of the top 15 most reported this year, including Cryptographic, Denial of Service, Command Injection, and Memory Corruption. New weakness types in the top 15 most reported include Insecure Direct Object Reference (IDOR), Brute Force, Server-Side Request Forgery (SSRF), and UI Redressing (Clickjacking).

Why are these vulnerabilities growing in number? What are the most impactful vulnerabilities that may not be in the OWASP Top 10? What's the top listing of vulnerabilities submitted by volume? Our analysis of the Top 10 most impactful vulnerabilities sheds light on these questions and more.


hackerone

VULNERABILITIES BY INDUSTRY

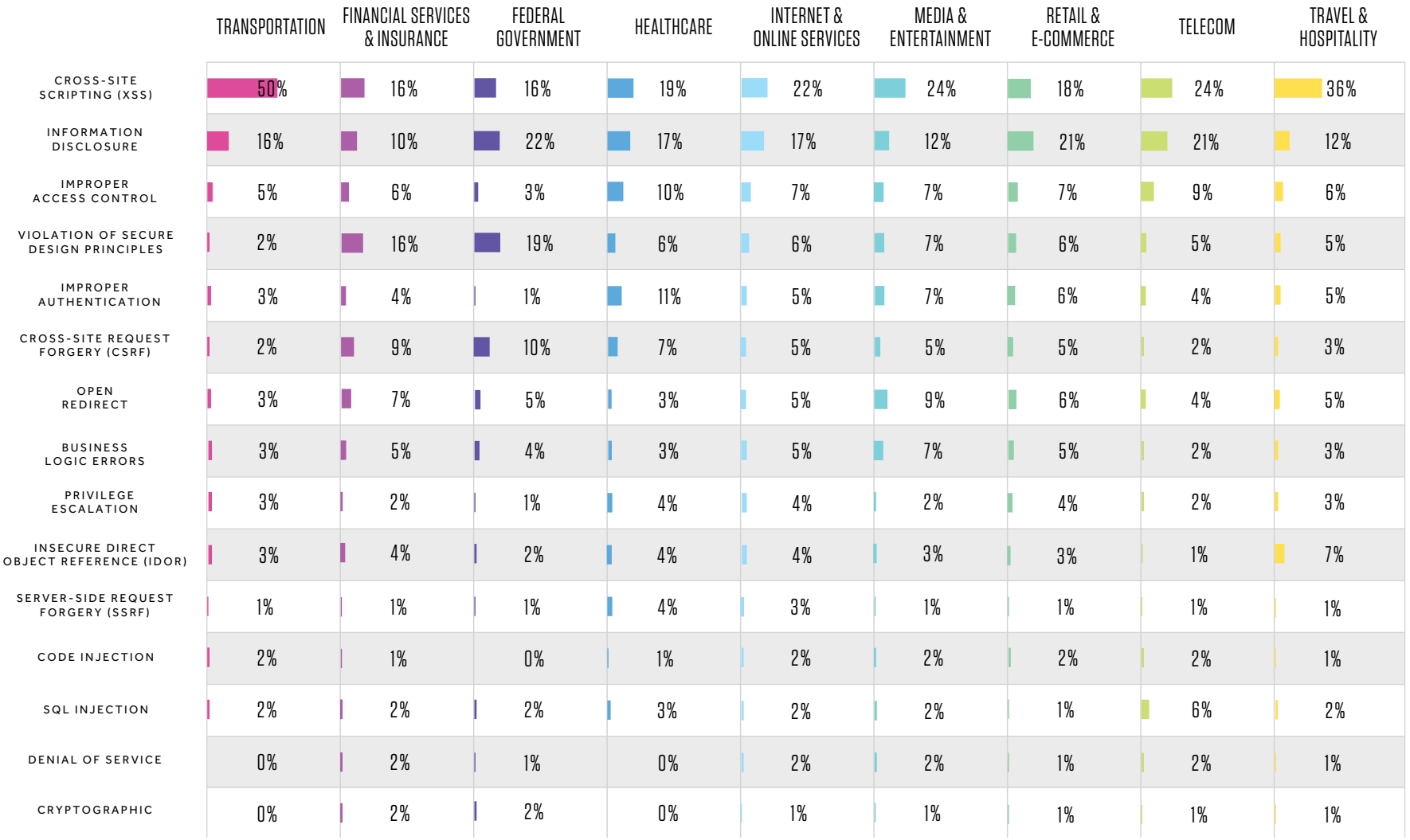
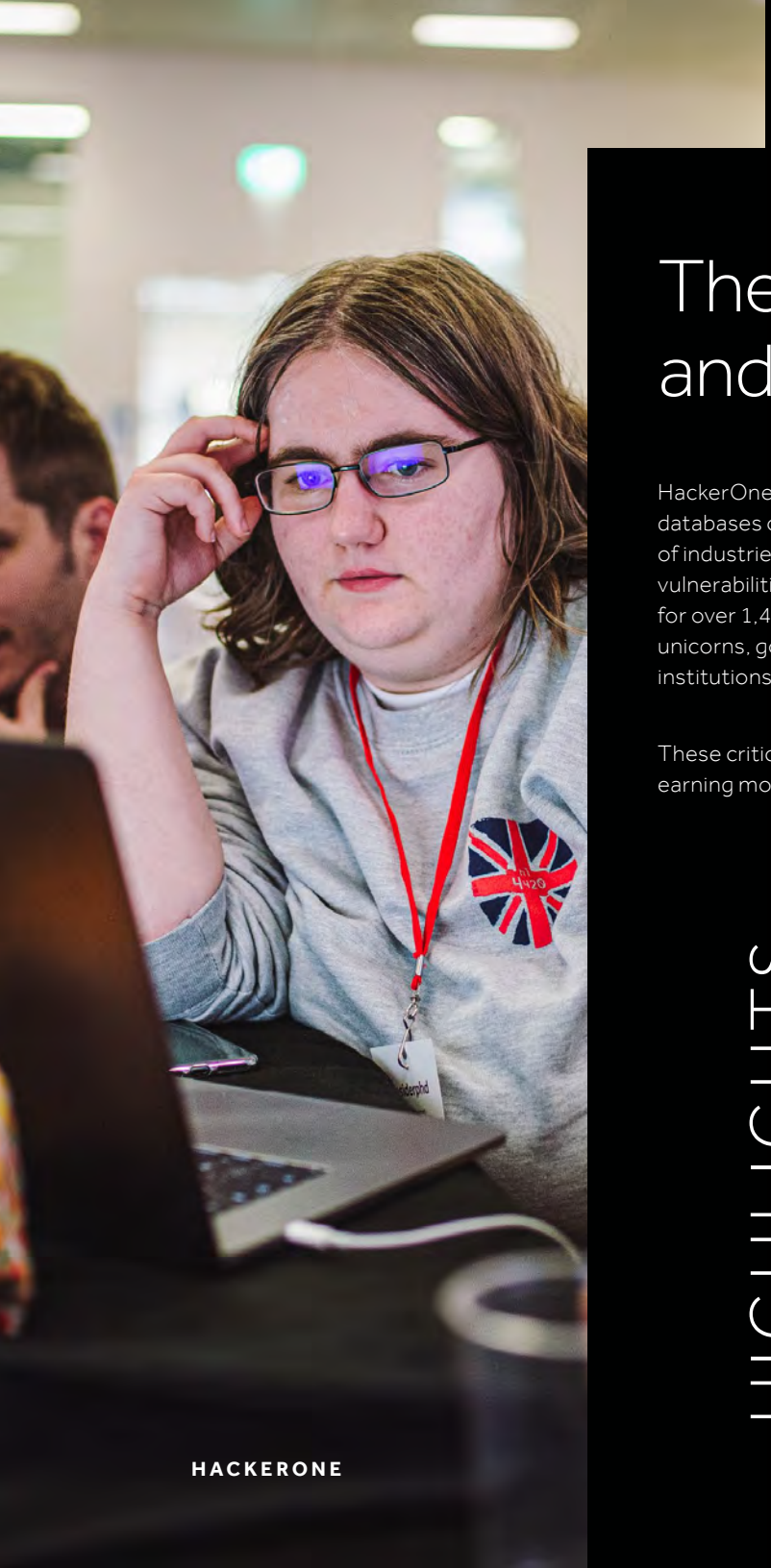


Figure 6: *The top 15 vulnerability types platform-wide, and the percentage of vulnerabilities received per industry.*



The HackerOne Top 10 Most Impactful and Rewarded Vulnerability Types

HackerOne has one of the largest and most robust databases of valid vulnerabilities from a broad array of industries and attack surfaces. These resolved vulnerabilities represent tangible risks that existed for over 1,400 organizations, including technology unicorns, governments, startups, global financial institutions, and open source projects.

These critical vulnerabilities contributed to hackers earning more than $62 million in bounties on the HackerOne platform to date. It also includes vulnerability types with the highest severity scores and total report volume by vulnerability type.

To learn more, visit the interactive microsite for The HackerOne Top 10 Most Impactful and Rewarded Vulnerability Types You'll be able to slice and dice data by industry, see how different vulnerability types are trending, and more.

HIGHLIGHTS

01 The technology world's mass migration to the cloud has resulted in increased risks from vulnerabilities like Server Side Request Forgery.

02 Despite the ever-growing attention on protecting user privacy and data, Information Disclosure vulnerabilities are still common.

03 Less than half of this year's Top 10 overlap with the OWASP Top 10.

04 Highly impactful vulnerabilities, like SSRF, IDOR, and Privilege Escalation, are harder to find but continue to be the most valuable vulnerabilities based on bounties awarded.

CUSTOMER SPOTLIGHT

“Responding quickly to researchers who report vulnerabilities is key to building relationships with them that benefit the bank.”

Goldman Sachs

Goldman Sachs just turned 150 years old. This global financial investment leader was built on a foundation of culture, history, and people that has allowed it to be nimble and successfully adapt to a frequently changing world.

In May 2018 Goldman Sachs became the first investment bank to launch a vulnerability disclosure policy. In the first year of their program, more than 23 vulnerabilities, each representing real world risk to their customers and data, were safely resolved.

Today, Goldman Sachs is working with hackers to identify vulnerabilities in their consumer websites, including goldmansachs.com and marcus.com, a site for consumer loans. On average, their internal security team has resolved vulnerability reports within two months, and have responded to bug reports in as little as one minute, further resolving reports within one hour.

Time to Resolution by Industry

Public bug bounty programs receive their first vulnerability report within the first 24 hours in 77% of the cases. For the U.S. Army, it only took five minutes. Once a customer has confirmed the vulnerability is valid, they have the opportunity to reward the hacker and fix the issue. HackerOne tracks the time-to-vulnerability resolution for all programs. A speedy resolution not only helps to quickly protect the organization and its customers by eliminating the vulnerability, it also helps attract hackers to the customer's program and is a key indicator of program health.

Our data demonstrates that the top performing programs on HackerOne (based on the HackerOne Success Index) attract not only more hackers but more repeat hackers. Repeat hackers are responsible for most resolved reports and bounties on the HackerOne platform. The more time a hacker spends looking at specific software, the more valuable the reports are likely to be. This indicates there is significant value in building hacker loyalty.

Looking at data across the HackerOne platform, the overall median time to resolution was 17 days, down from 22 days in the previous year. Consumer Goods was the fastest at resolving vulnerabilities in just two days. Rounding out the top 5 fastest were Cryptocurrency & Blockchain (seven days), Healthcare (11 days), Financial Services & Insurance (12 days), and Professional Services tied with Media & Entertainment (12 days).

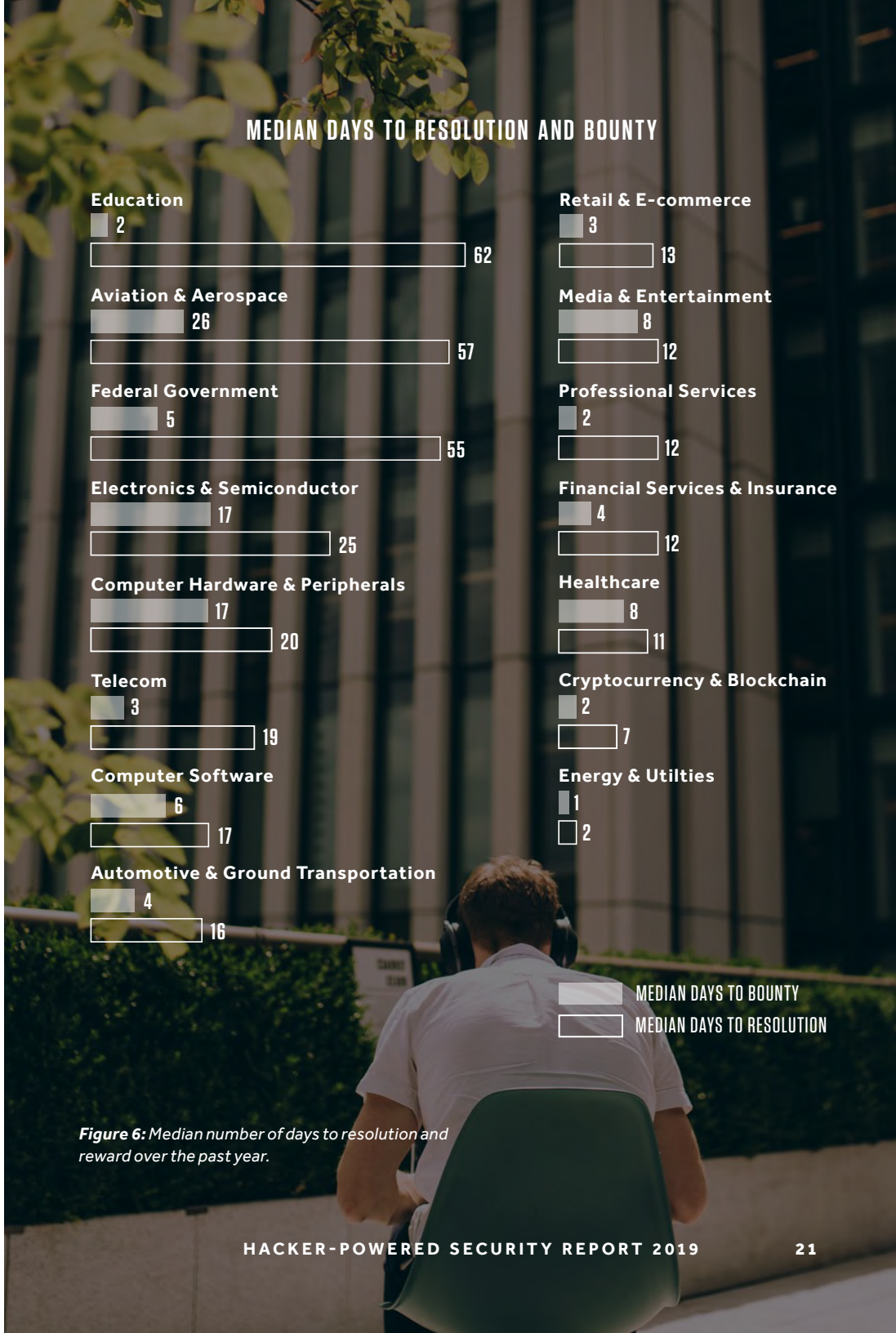


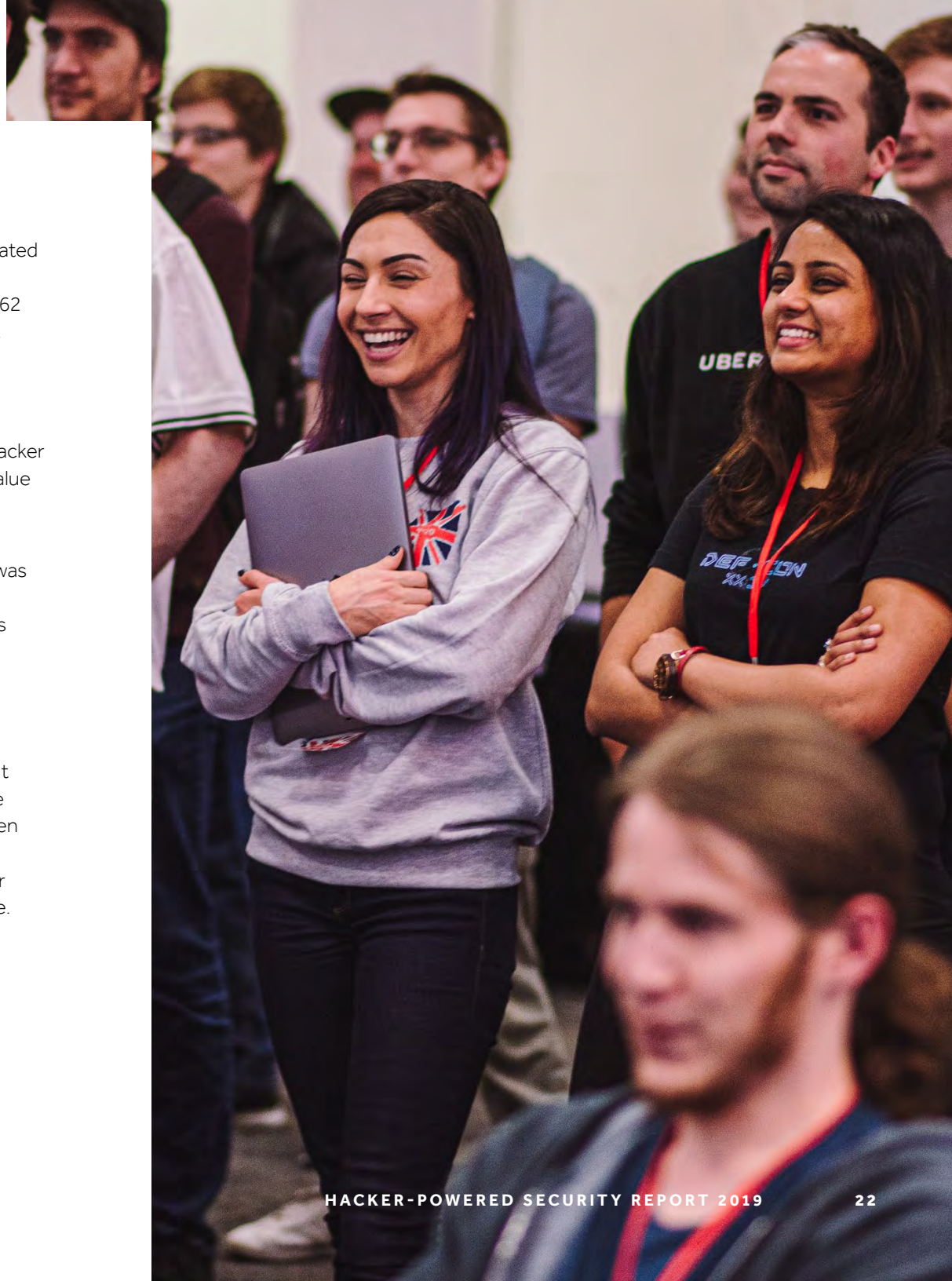
Figure 6: *Median number of days to resolution and reward over the past year.*

Industries resolving issues more slowly are those in highly regulated areas with complex software stacks and/or integrated supply chains. At the other end of the speed spectrum are Education (62 days), Aviation & Aerospace (57 days), and Federal Government (55 days).

Once an issue is resolved, a bounty should be paid shortly thereafter—if not at the time of validation. This ensures both hacker satisfaction and that the payment process is aligned with the value provided by the hackers who identify the vulnerabilities.

The industry with the fastest median days to bounty payment was Local Government (< one day). Consumer Goods, Professional Services, and Education all had a median time-to-bounty of less than two days. The industries with the slowest days to bounty payment are Aviation & Aerospace (26 days), Electronics & Semiconductor (17 days), and Computer Hardware (17 days).

All industries tend to pay hackers before issues are resolved (but after they are validated), which reflects the value they see in the hackers' work. Hackers appreciate speedy award payments when their work is done. More organizations are also starting to re-engage hackers after an issue has been resolved, soliciting their help to validate that a fix does indeed resolve the reported issue.



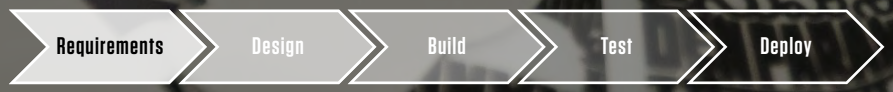


Figure 7: *A generic software development lifecycle.*

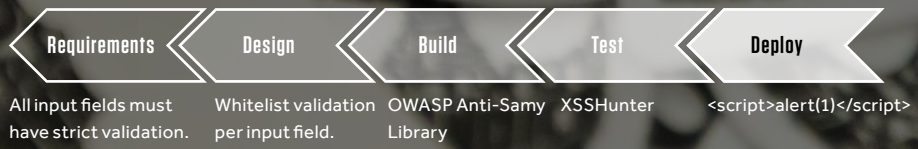


Figure 8: *A bug bounty lifecycle at Verizon Media, showing how a bug report can be worked upstream to impact every stage of software development. Graphic courtesy of Verizon Media's The Paranoids.*

Flip the Script, Think Like a Hacker

Verizon Media's security team refers to themselves as The Paranoids. They secure the data of more than 1 billion users across dynamic brands such as Yahoo!, AOL, and TechCrunch. The team uses hacker-powered security to help integrate their security program into their software development lifecycle (SDLC) in a novel way.

Typically, security teams work to fix the offending code behind a valid bug report and the story ends there. The Paranoids, however, view that as just the beginning. The team frequently uses the bug as a new test case. As more bugs of a particular type are reported, they work with their product developers to build a new library into the codebase. They even go so far as to work with their architects to design new controls when appropriate.

The result is a collection of lessons learned for every class of vulnerability, which they then use to create requirements, policies, or standards to address it.

Bounty Trends: Severity

The median value paid for critical vulnerabilities on HackerOne was $2,000, which is up 60% from the $1,250 median in 2017. As organizations fix more vulnerabilities and harden their attack surface, bounty values naturally increase over time, since vulnerabilities become more difficult to identify, thus requiring more skill and effort to discover.

The average bounty paid for critical vulnerabilities across all industries on HackerOne rose to $3,384 in the past year. That's a 48% increase over last year's average of $2,281 and a massive 71% increase over the 2016 average of $1,977.

Vulnerabilities by Severity

Critical vulnerabilities accounted for just over seven percent of all reports. The share of the most impactful bugs—critical and high combined—increased for the third year in a row, from 22% in 2016 to 24% in 2017 and to 25% this year.

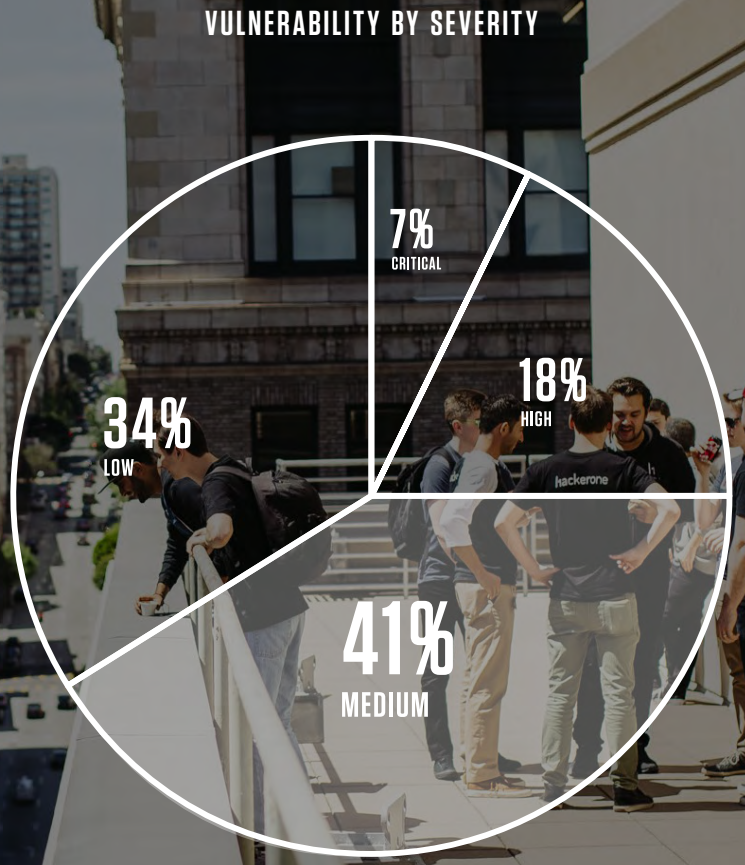


Figure 9: *The percentage of all vulnerabilities that are categorized as critical, high, medium, or low severity.*

Average Bounty Payout Per Industry for Critical Vulnerabilities

The highest average bounty payment by industry for critical issues come from Cryptocurrency & Blockchain ($6,124), Internet ($4,973), and Aviation & Aerospace ($4,500). Those are all significantly higher than the platform average of $3,384.

For all vulnerabilities reported of any severity, the average bounty payout was $771, up 65% from $467 last year.

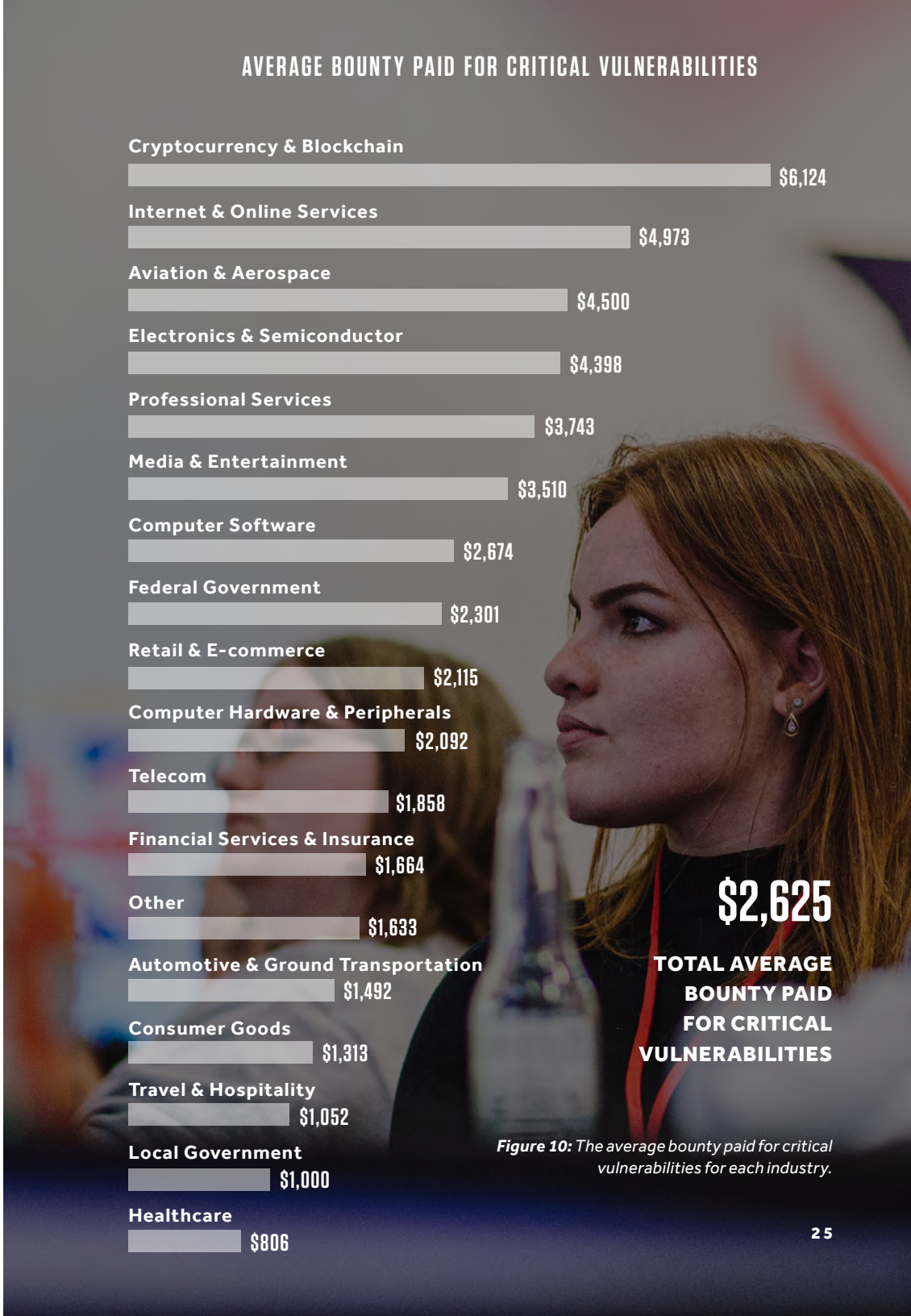


Figure 10: *The average bounty paid for critical vulnerabilities for each industry.*

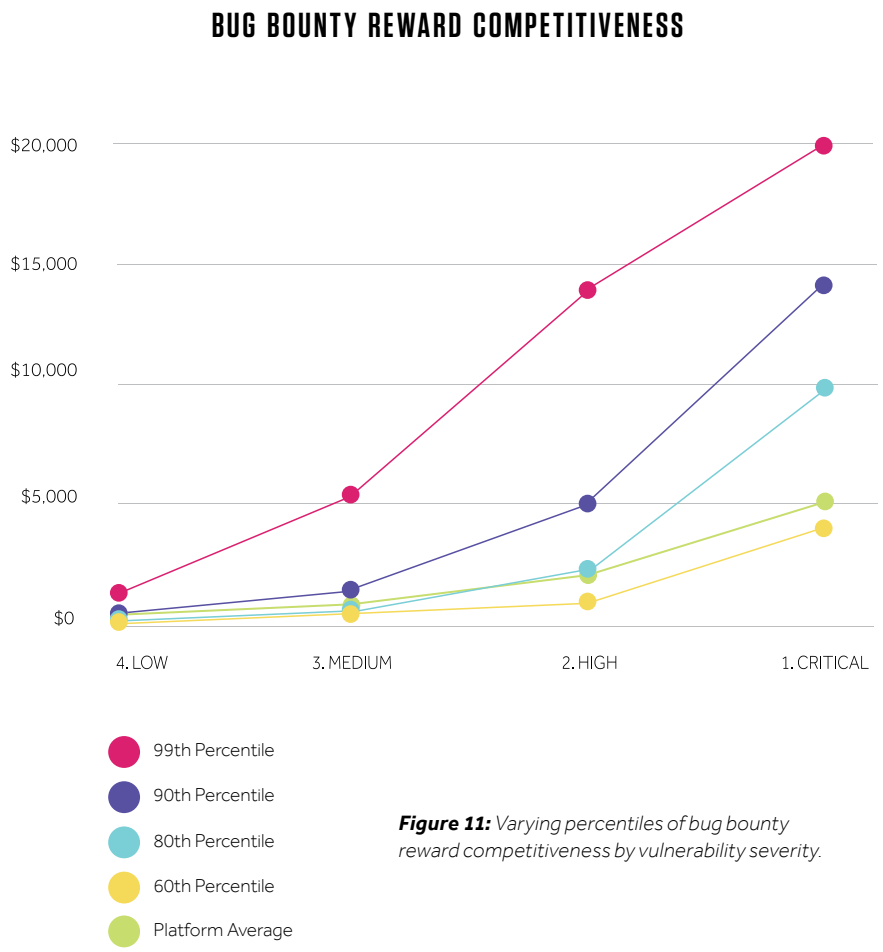


Figure 11: *Varying percentiles of bug bounty reward competitiveness by vulnerability severity.*

Bounties by Severity

High-performing bug bounty programs are paying top dollar to attract the best talent to uncover more critical vulnerabilities. Bounty programs on HackerOne that reward an average of $20,000 for critical vulnerabilities are in the top 1% of reward competitiveness, which remained the same from last year's average bounties paid for critical vulnerabilities. To date, $100,000 remains the largest individual bounty earned for a critical vulnerability on HackerOne. There have been multiple awards at this value, most notably by Intel, which awarded $100,000 for the discovery of a new Spectre variant.

In comparison, 60% of organizations on the platform award $4,000 on average for critical vulnerabilities—up from just $1,000 last year.

Bug bounty programs will pay at or below average bounties when they first launch. As the organization fixes more vulnerabilities and their attack surface hardens, bounty payouts should increase over time. In most cases, critical vulnerabilities are harder to find in an organization that pays $30,000, for example, than in an organization that pays $5,000.

Hardening your attack surface, increasing reward competitiveness, and reducing your risk takes time and sustained effort. Bug bounty programs offering bounties in the top 1% get there by continuously working with hackers to improve security.

CUSTOMER SPOTLIGHT

PayPal

“Security has always been a top priority for our business, ingrained into the fabric of everything we do.”

PayPal

“The security team for PayPal’s digital payments platform is tasked with protecting the financial and personal information of 267 million active accounts, in more than 200 markets around the world,” says Ray Duran, Information Security Engineer at PayPal. “Security has always been a top priority for our business, ingrained into the fabric of everything we do.”

PayPal has been running their bug bounty program since 2012. In 2018, they joined HackerOne and instantly increased their community of hackers from 2,000 to over 300,000. In the first six months, they received vulnerability reports from 890 researchers across 56 countries, compared to 365 researchers in the prior six months.

“In addition to being able to work with a broader more diverse set of researchers, HackerOne has enabled us to process bounty awards for qualifying submissions faster and get direct feedback from researchers on how to further improve our program,” said Duran. PayPal’s top bounty award recently increased to $30,000 for a critical remote code execution (RCE) vulnerability.

In April 2019, PayPal crossed the $1 million milestone in bounties. At the same time, they moved all of their payments to HackerOne to easily reward hackers in their own country’s currency.

Bounty Trends: Top Awards

From 2012 through May 2019, organizations awarded hackers more than $51 million. Nearly half of that, $23.5 million, was awarded in the past year alone.

Enterprise businesses worldwide are eager to compensate hackers for their work. Apple, Google, Intel, Microsoft, and other leading organizations offer seven-figure awards for vulnerabilities. It's not uncommon for even smaller companies to offer bounties in the tens of thousands of dollars for critical security vulnerabilities.

The highest bounty paid in the past year remains $100,000. Organizations in the Cryptocurrency & Blockchain, Media & Entertainment, Technology, and Telecommunications industries all awarded top bounties of $20,000 or more. Across all industries, 511 bounty awards in excess of $10,000 were paid over the past year. That's up 340% from the 116 bounties of this size awarded in the previous year.

Figure 12: *The top bounty awarded in the past year on the HackerOne platform by industry.*

BOUNTY AWARDS BY INDUSTRY

Figure 13: *The total bounties paid in the past year by each industry category on the HackerOne platform.*

CUSTOMER SPOTLIGHT

“Our HackerOne bug bounty program has one of the most permissive scopes in the industry.”

Dropbox

In April 2019, HackerOne kicked off Singapore’s first live hacking event (h1-65) with leading global collaboration platform Dropbox. Over the course of 8 hours, 39 hackers reported 264 vulnerabilities, which earned them $336,479 in bounties.

“Dropbox invests heavily to build a security team comprised of the best talent in the industry,” says Rajan Kapoor, Director of Security at Dropbox. “Our HackerOne bug bounty program has one of the most permissive scopes in the industry. This allows us to work with security researchers to test the broadest attack surface possible. The impressive contributions from the community have made Dropbox, and the Internet as a whole, a safer place.”

Dropbox is recognized as an industry leader in the security field. Their engineers regularly contribute to security research and share best practices, and the company launched their public bug bounty program in January 2015. Since then, the team has paid out more than $1 million in bounty awards and resolved over 250 vulnerabilities thanks to the work of nearly 200 hackers.

But for h1-65, they wanted to do something new. At this live hacking event, Dropbox opened up its core properties for testing, but also added newly-acquired HelloSign to the event’s scope. Dropbox firmly believes this progressive approach to hacker-powered security should be an industry standard. This comprehensive approach to security helps ensure increased product security as well as upstream security for products you integrate with.

To learn more about our live hacking events, visit hackerone.com/live-hacking.

Signal-to-Noise Ratio

Signal-to-noise is a measure of a program's submission quality based on the validity of incoming reports. Signal indicates the number of valid reports received, whereas noise is the share of non-valid reports received. Today HackerOne delivers an 81% platform-wide signal. A higher signal-to-noise ratio means more valid reports are received and less time and resources are spent on identifying invalid reports.

In the early days of hacker-powered programs, many organizations had to deal with a low signal-to-noise ratio before the program could be deemed a success. Do-it-yourself bug bounty programs that don't benefit from noise-reducing platform features can experience signal-to-noise ratios as low as 4%.

Today, with platform automation, smart algorithms, hacker signal data, and trained professionals on-demand, that ratio can approach 100%. This lowers the total cost of ownership for hacker-powered security and puts it within reach of any security budget.

HackerOne Services help many customers augment their internal security team to act quickly and effectively on vulnerability reports. With proper end-to-end management, bug reports are swiftly evaluated, hackers are engaged, and above all, the risk of a security incident is reduced. HackerOne Services can evaluate all incoming reports, manage communications with hackers, and even package and deliver valid vulnerability reports in any format.

Delivering the best signal-to-noise ratio in the bug bounty industry means customers save a lot of time, freeing up valuable team resources to focus on more impactful tasks. False positives are a reality for many security products, but they are no longer a significant concern with hacker-powered security.

CLEAR SIGNAL

Vulnerability reports closed as "Resolved." This means the issue was a unique, valid security bug that was fixed by the vulnerability response team.

NOMINAL SIGNAL

These reports are closed as "Informative" or duplicates of resolved issues. While not contributing to clear signal, many of these reports were technically accurate based on the best information available to the researcher.

NOISE

These reports are closed as "Not Applicable," "Spam," or duplicates of these types. This represents the noise in the signal to noise ratio.

PLATFORM AUTOMATION AND SMART ALGORITHMS

HackerOne's set of crowdsourced vulnerability data results in unrivaled machine learning algorithms. In January 2018, we announced Human-Augmented Signal, which improves the signal of programs significantly and automatically. How does it work? Our system utilizes various criteria to automatically classify all incoming reports and reports with potential noise are forwarded to HackerOne security analysts for review. This human-in-the-loop review guards against false positives and further trains our machine learning classifiers.

TRACKING HACKER SIGNAL

The HackerOne Platform allows you to privately invite a select group of hackers to test your platform in a safe and controlled manner. Hacker activity and productivity is tracked in three main ways: Reputation, Signal, and Impact. Signal measures average report validity, Impact measures average report severity, and Reputation is a cumulative measure of Signal and Impact. These scores can be used as a filter for determining which hackers are invited to your private programs or to serve as an initial method for evaluating incoming reports.

EXPERT TRIAGE AND SERVICE

Since 2016 HackerOne has been offering our customers managed services, which includes full triage and bug bounty program management to serve as the most convenient option for resource constrained organizations. Managed programs on HackerOne consistently garner higher Clear Signal (40%) than unmanaged programs (33%) on HackerOne. HackerOne Triage is the practice that takes Signal up to 100%.

We've set a goal to reach 90% signal—a standard that hasn't been seen on any other platform in our industry. Currently, HackerOne consistently maintains 81% signal platform-wide.

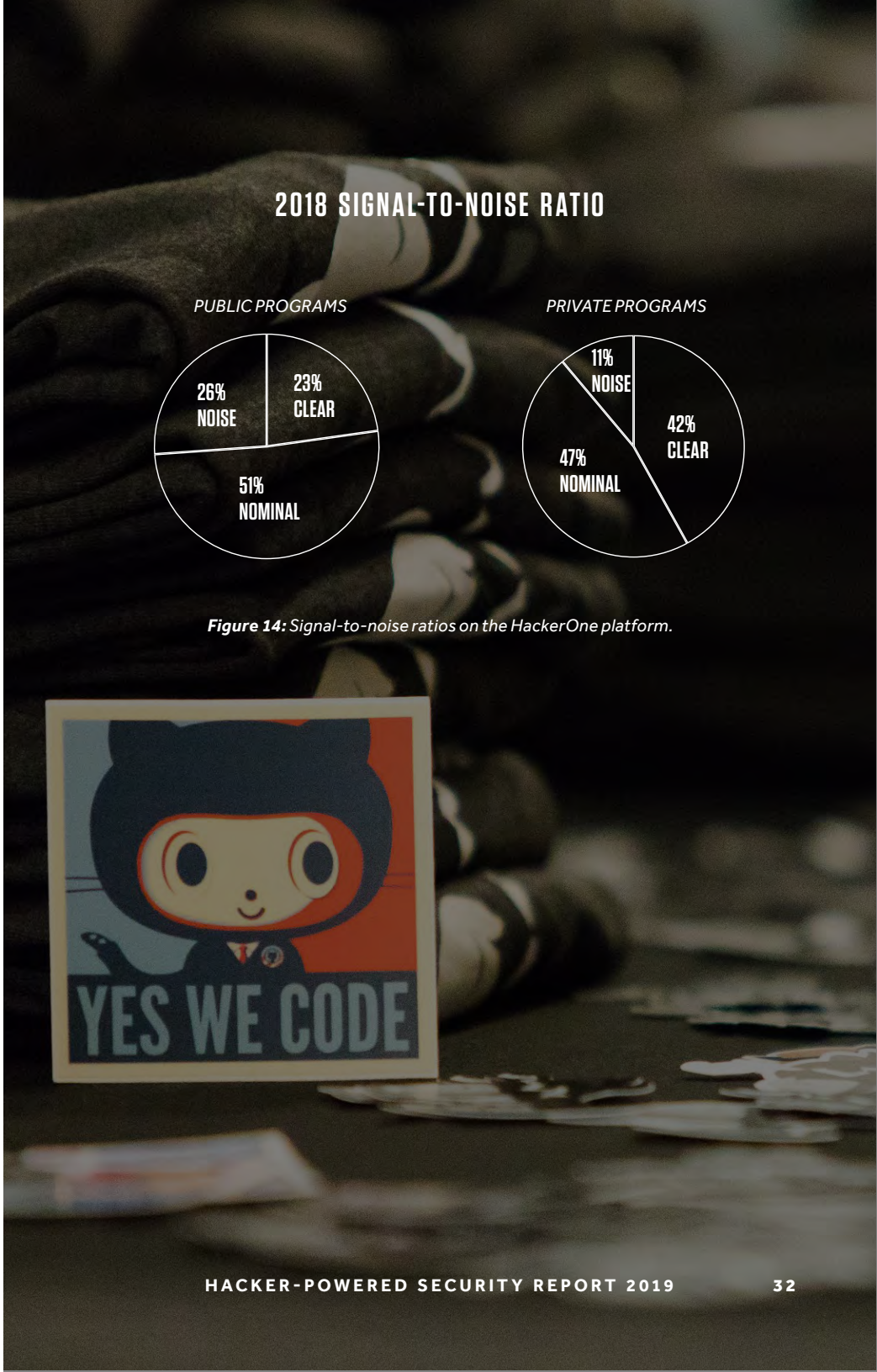


Figure 14: *Signal-to-noise ratios on the HackerOne platform.*


hackerone

Working with Vetted, Trusted Hackers

Private programs give you complete control over which hackers are invited and who is eventually approved to participate in your program. HackerOne provides several layers of control for selecting, inviting, and approving hackers based on their HackerOne Reputation metrics, past program participation, specific skills, and more.

HackerOne makes it easy so you can spend more time resolving the vulnerabilities hard-working hackers identify. Here's how it works:

01 You identify and select hackers based on their activity on other bounty programs, as well as their Signal, Impact, and Reputation scores. These scores track hacker activity and submission quality, resulting in an individual Reputation score. By looking for those who have experience on similar technologies, and who are high performers, you can narrow down your list of potential participants.

02 HackerOne helps you further narrow your list by finding hackers with the skills you need. Each hacker's profile page contains their "Hacktivity," which shows all of their previously resolved reports and includes their number of bugs found, thanks received, and badges earned. This offers a unique view into the skills and experience of each hacker and, if public, the details of the actual reports. Hackers can also add skills to their profile, which require them to submit relevant reports.

03 Your HackerOne Program Manager works with you to develop your program's custom requirements, which might include a robust application process, and even background checks.

If you're looking for even more scrutiny over potential participants, you need HackerOne Clear. HackerOne Clear hackers meet the strictest background and identity standards of the most demanding global organizations, such as the U.S. Department of Defense. Contact us to learn more.

Vulnerability Disclosure Policy Adoption

Say someone discovers a critical security flaw impacting your customers. Would you want your team to know about it, no matter the source? A vulnerability disclosure policy (VDP), commonly referred to as the "see something, say something" of the internet, is an organization's formalized method for receiving such vulnerability submissions from the outside world. The VDP instructs hackers on how to submit vulnerability reports, and defines the organization's commitment to the hacker on how reports will be handled. The practice has been defined by the U.S. Department of Justice (DoJ) and in ISO 29147.

Known by some as Responsible Disclosure Policies, they have resulted in global organizations detecting vulnerabilities impacting hundreds of millions of consumers. In just three years, the U.S. Department of Defense has detected more than 10,000 security vulnerabilities through their VDP program alone. Unlike a bug bounty program, VDPs do not offer incentives or rewards for vulnerability reports.

Despite the effectiveness of these programs, only **93% of the world's top companies on the Forbes Global 2000 do not offer a means for contacting them to disclose a critical vulnerability.** This number is unchanged from last year.

There are 5 critical elements to a VDP, one of which is creating a safe harbor for hackers. In March 2018, Dropbox added a legal safe harbor pledge to its VDP, promising "to not initiate legal action for security research conducted pursuant to the policy, including good faith, accidental violations." Dropbox then made its VDP "a freely copyable template" for others to follow their lead. HackerOne also introduced legal safe harbor language as a default for new policy pages, further solidifying it as industry standard.

HackerOne Response is our turnkey solution offering enterprise-grade security and conformance with ISO-29147 (vulnerability disclosure) and ISO-30111 (vulnerability handling). It allows vulnerability management teams to work directly with external third-parties to resolve critical security vulnerabilities before they can be exploited. HackerOne Response is a single solution that helps you simplify your disclosure process, reduce risk across your organization, and avoid the unpleasant surprise of an unknown vulnerability going public or getting exploited.

5 CRITICAL COMPONENTS FOR EVERY VDP

01 **PROMISE**
Demonstrate a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities.

02 **SCOPE**
Indicate what properties, products, and vulnerability types are covered.

03 **"SAFE HARBOR"**
Assures that reporters of good faith will not be unduly penalized.

04 **PROCESS**
The process finders use to report vulnerabilities.

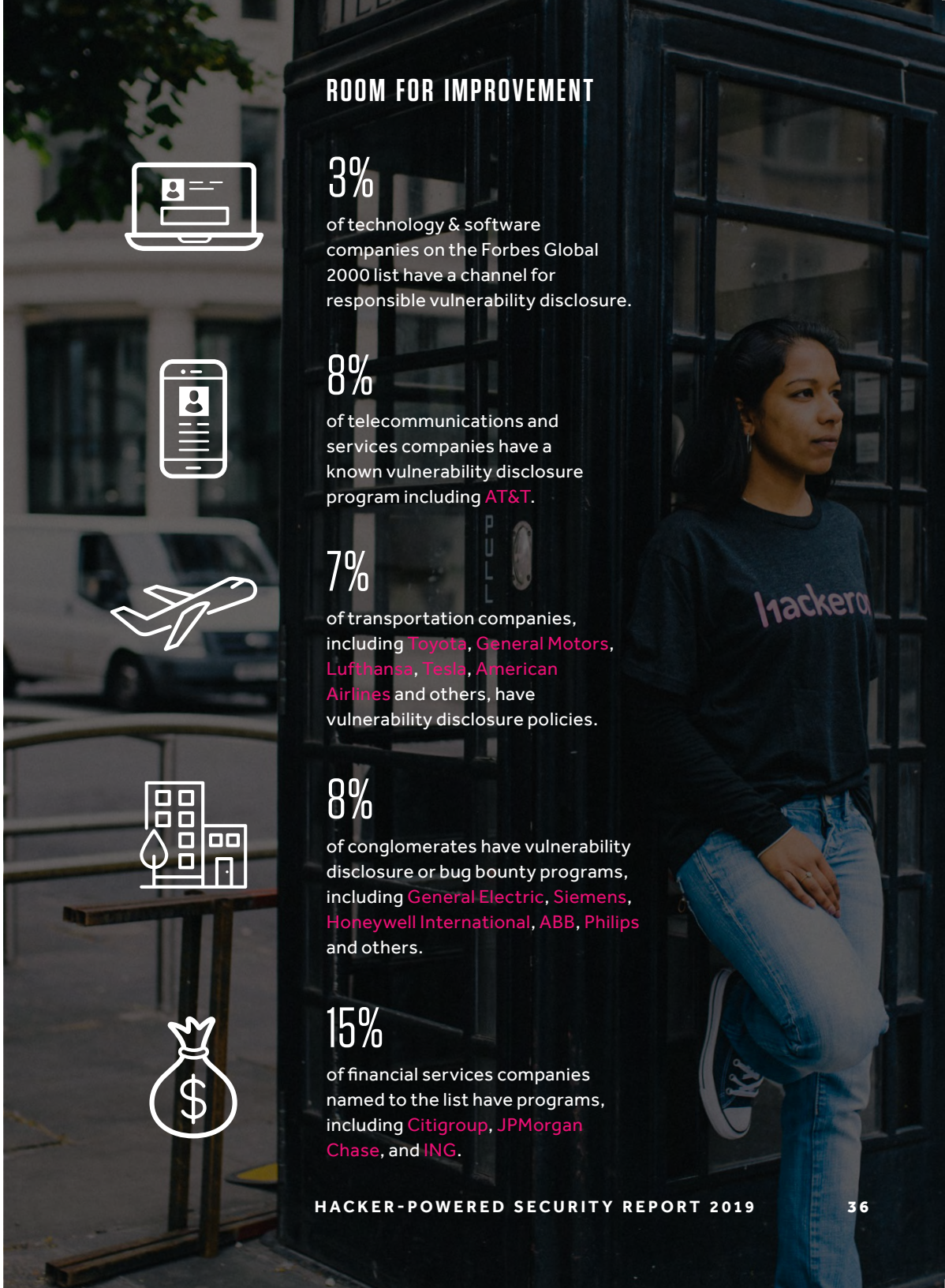
05 **PREFERENCES**
A living document that sets expectations for preferences and priorities regarding how reports will be evaluated.

Forbes Global 2000 Breakdown

Each year, HackerOne analyzes the Forbes Global 2000 list of the world's most valuable public companies as one benchmark for public vulnerability disclosure policy adoption. Based on the 2017 Forbes Global list, **93% of the Forbes Global 2000 do not have a known vulnerability disclosure policy**, compared to 94% of the 2016 list.

While these numbers have significant room to improve, organizations are pushing for more progress. The VDP Framework recommended by the DoJ, is one example. Gartner's recent predictions that crowd-sourced security solutions will be employed by more than 50% of enterprises by 2022, up from less than 5% today, shows that more organizations are starting to see the value.

This progress is critical to reducing risk, as nearly **1 in 4 hackers have not reported a vulnerability that they found** because the company didn't have a channel to disclose it. Having a VDP in place reduces the risk of a security incident and places the organization in control of what would otherwise be a chaotic workflow.



ROOM FOR IMPROVEMENT

3%

of technology & software companies on the Forbes Global 2000 list have a channel for responsible vulnerability disclosure.

8%

of telecommunications and services companies have a known vulnerability disclosure program including AT&T.

7%

of transportation companies, including Toyota, General Motors, Lufthansa, Tesla, American Airlines and others, have vulnerability disclosure policies.

8%

of conglomerates have vulnerability disclosure or bug bounty programs, including General Electric, Siemens, Honeywell International, ABB, Philips and others.

15%

of financial services companies named to the list have programs, including Citigroup, JPMorgan Chase, and ING.

Voices of Vulnerability Disclosure

Quotes from business and government leaders on why you need a vulnerability disclosure policy in place today to detect where you are most vulnerable.

To improve the security of their connected systems, every corporation should have a vulnerability disclosure policy that allows them to receive security submissions from the outside world.

JEFF MASSIMILLA
Chief Product Cybersecurity Officer, General Motors

A VDP should be considered table stakes for any company with a public footprint.

SCOTT CRAWFORD
Research Director of Information Security, 451 Research

We need to move to a world…where all companies providing internet services and devices adhere to a vulnerability disclosure policy.

JULIAN KING
Security Union Commissioner, European Commission

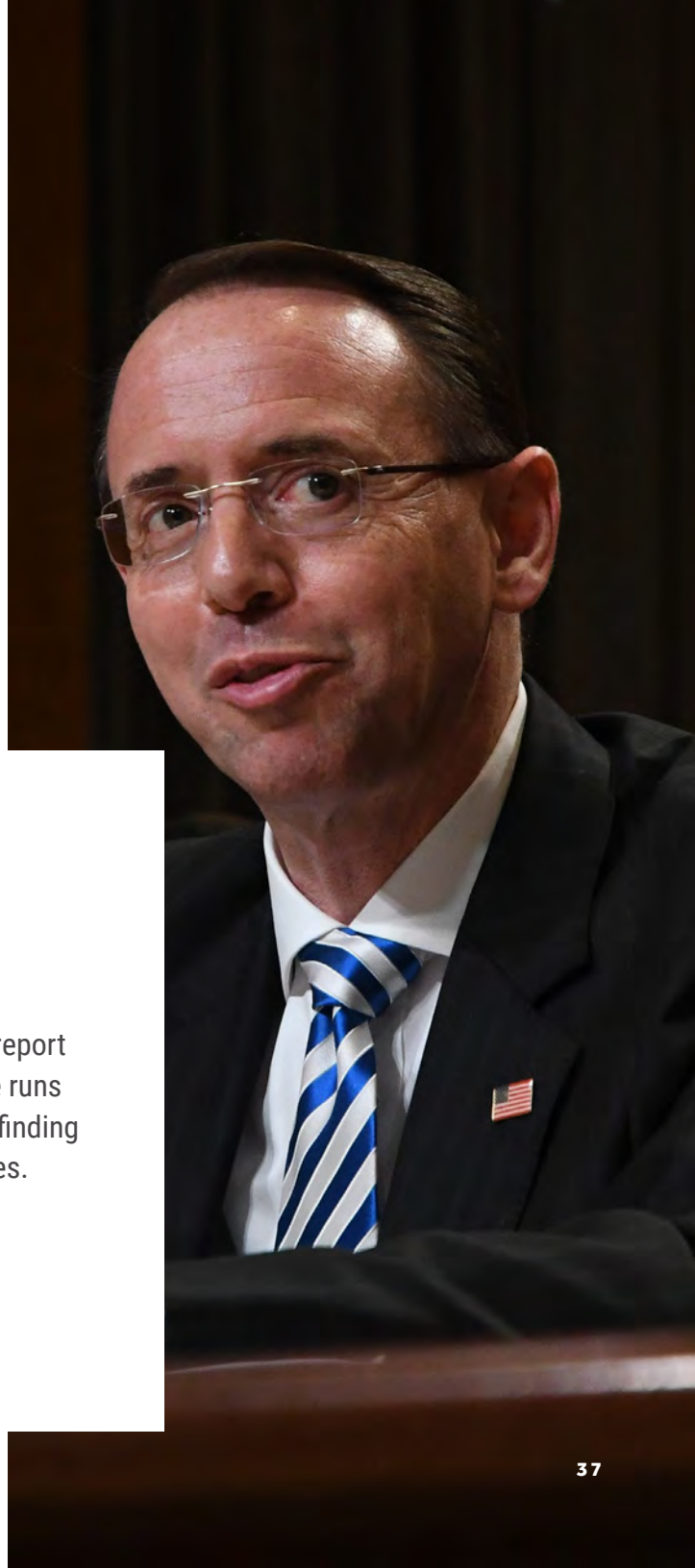
Like many companies, we have a responsible disclosure program which provides an avenue for ethical security researchers to report vulnerabilities directly to us.

CAPITAL ONE

“

All companies should consider promulgating a vulnerability disclosure policy, that is, a public invitation for white hat security researchers to report vulnerabilities. The U.S. Department of Defense runs such a program. It has been very successful in finding and solving problems before they turn into crises.

ROD J. ROSENSTEIN
Former Deputy Attorney General, U.S. Department of Justice



Manufacturers should also adopt a coordinated vulnerability disclosure policy and practice that includes acknowledging receipt of the vulnerability to the vulnerability submitter within a specified time frame.

U.S. FOOD AND DRUG ADMINISTRATION
Postmarket Management of Cybersecurity in Medical Devices

I think a disclosure program, and going a step further, a bug bounty program, are tools available. In the right circumstances, I like those tools.

NICK RITTER
VP Product Security, General Electric

"

Companies should communicate and coordinate with the security research community as part of a continuous process of detecting and remediating software vulnerabilities. Given the complex nature of software, security-related bugs are inevitable, and the research community represents a critical tool in defending against the exploit of such vulnerabilities. Studies have found that the adoption of vulnerability disclosure policies represents a cost-effective and efficient method of identifying and addressing vulnerabilities.

FEDERAL TRADE COMMISSION

Look who is talking about vulnerability disclosure and read more.

CUSTOMER SPOTLIGHT

“Due to its success over the past two years, the program grew to include expanded vulnerability criteria and increased payouts in 2018.”

Google Play

In October 2017, Google and HackerOne introduced the Google Play Security Reward Program, the first and only vulnerability rewards incentive program for an app ecosystem. Developers of popular Android apps were invited to start hacker-powered security programs on HackerOne, with Google Play providing a bonus reward of $1,000 on qualifying vulnerabilities.

As more developers opted-in, more apps were listed. Due to its success over the past few years, the program grew to include expanded vulnerability criteria and increased bonuses in 2018. In mid-2019, bonus awards for remote code execution bugs increased from $5,000 to $20,000, and theft of insecure private data and protected app component awards increased from $1,000 to $3,000. And that’s on top of any bounties for disclosing vulnerabilities to participating app developers.

“As the Android ecosystem evolves, we continue to invest in leading-edge ideas to strengthen security,” says Vineet Buch, former Director of Product Management at Google Play. “Our goal is to continue to make Android a safe computing platform by encouraging our app developers and hackers to work together to resolve unknown vulnerabilities. We are one step closer to that goal.”

The results have been inspirational, with $201,000 in total bounty bonuses paid across 118 resolved reports. The program has triggered an influx of ecosystem providers building out their cybersecurity strategies to include bug bounty programs. Other ecosystems are also starting programs on HackerOne, including open-source publishing platform WordPress and Salesforce, which lists their VDP on HackerOne.

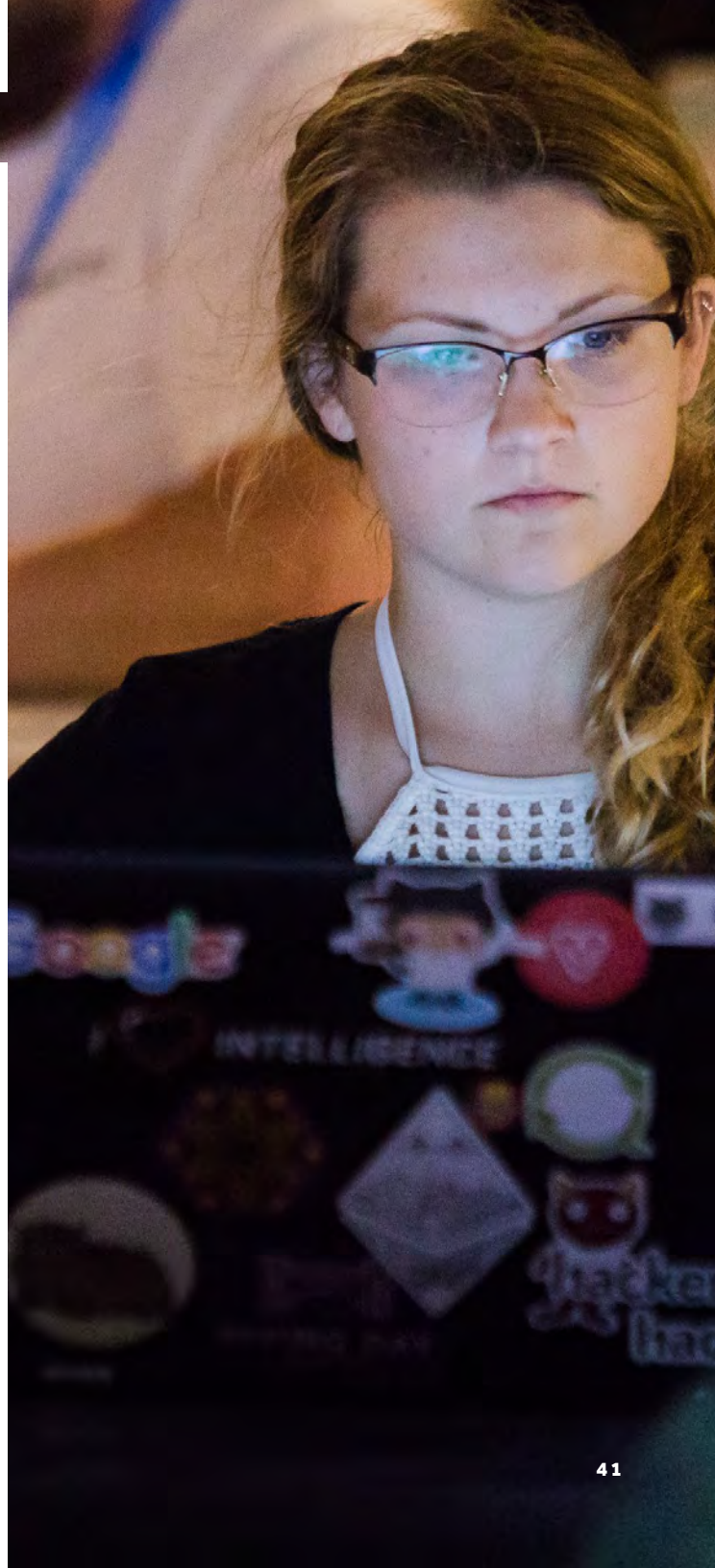
Evolution of Hacker-Powered Policy

U.S. legislators have realized the benefits of working with hackers following the success of the Hack the Pentagon crowdsourced security initiative that began in 2016. Federal support for hacker-powered security as a best practice comes from Federal Trade Commission, Food and Drug Administration, and National Highway Traffic Safety Administration. Legislators have started to take action, introducing bills that incorporate hacker-powered security such as Hack the Department of Homeland Security and Hack the State Department.

Key legislative initiatives this year include the passage of the Secure Technology Act (H.R. 7327) and the National Defense Authorization Act for Fiscal Year 2020 (NDAA), which would require federal agencies to utilize VDPs and conduct security testing through crowdsourced platforms. The Hack Your State Department Act was also introduced in the U.S. Senate, requiring the agency to establish a VDP and a bug bounty program to identify and report vulnerabilities of Internet-facing information technology of the Department of State.

The National Institute of Standards and Technology (NIST) is also pioneering hacker-powered policies with their voluntary framework for managing risks related to cybersecurity. It's designed to promote the protection of infrastructure and industries critical to the nation's economy and national security. In June 2019, NIST offered a draft white paper for public comment that explicitly points to the benefits of hacker-powered security. The draft implores organizations to gather information on potential vulnerabilities from "consumers and public sources," investigate all credible reports, and even establish a program to "make it easy for security researchers to learn about your program and report possible vulnerabilities."

Internet of Things (IoT) security for consumer devices has also been a hot topic among lawmakers around the world. The U.K. government proposed new IoT security legislation that would better secure the hundreds of thousands of devices that consumers have connected to the Internet, including a requirement to establish a VDP. The U.S. Senate Homeland Security and Government Affairs Committee advanced the Internet of Things Cybersecurity Improvement Act to establish cybersecurity standards for federal devices that are connected to the internet, including the requirement of coordinated vulnerability disclosure.



The government of Singapore remains a leader in hacker-powered security. In addition to programs run by their Ministry of Defense and Government Technology Agency, the Cyber Security Advisory Panel (CSAP) of the Monetary Authority of Singapore (MAS) recommended financial institutions adopt bug bounty programs as part of their cyber testing.

Lawmakers are also continuing to invite expert testimony on the use of ethical hackers and bug bounty programs. For example, in February, 2018, HackerOne joined other industry leaders and testified in front of the U.S. Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security. In June 2019, based on the testimony of HackerOne, Canada's House of Commons Standing Committee on Public Safety and National Security acknowledged the importance of VDPs in the financial services industry.

As more governments take more steps to regulate and mandate Internet and data security, HackerOne continues to promote responsible policies that support, not undermine, secure systems.

Enabling Compliance with Hacker-Powered Penetration Tests

Penetration tests are a staple of nearly every security program. They have been used for decades as a viable means for evaluating the security of a specific scope of technology. Traditional testing remains a necessary exercise to identify weaknesses and for compliance, but they are limited in that they provide only an occasional, point-in-time view of risk. With a hacker-powered pentest you can begin testing in days and reduce the risk of a security incident while achieving PCI DSS and SOC2 Type II compliance certifications.

> This is value that we never got from a pentest. Traditional pentests are not enough for modern day security.
>
> **GEORGE GERCHOW**
> *Chief Security Officer, Sumo Logic*

Crowdsourced pentests are becoming an increasingly common and effective means for a continuous, proactive security testing and broad investigation of a technology's security risks. Whereas traditional testing can aim a small talent pool at a specific scope for a few weeks, hacker-powered pentests can bring thousands of researchers with varying skills and broad approaches. What's more, they offer the benefit of paying for validated results rather than effort.

The hacker-powered pentest methodology, enabled via HackerOne Challenge, uses a hybrid model that combines incentive-driven vulnerability testing with targeted testing for specific categories of vulnerabilities. This ensures diversity in testing, realistically simulates real-world attacks, emphasizes the discovery of exploitable, impactful, vulnerabilities, and promotes the use of the most modern testing tools and techniques.

A recent Total Economic Impact (TEI) report from Forrester Consulting found that a **HackerOne Challenge eliminated $156,784 in total costs** and reduced internal security and application development efforts, **saving an additional $384,793 over three years**. The TEI also found that organizations using a HackerOne Challenge to augment traditional pentests reduced the likelihood of a security breach by finding more vulnerabilities faster. It also led to higher customer satisfaction and retention, since it increased customer confidence in the company's ability to securely provide services.

> We turned to HackerOne for scalable real-time testing that would look in the places we weren't looking—not a simulation or templated test—for SOC 2 compliance.
>
> **STEVE SHEAD**
> *Vice President InfoSec & IT, Grand Rounds*

Hacker-powered pentests combine all the benefits of hacker-powered security with the requirements of PCI DSS, SOC2 Type II compliance frameworks.

Organizations across various industries are already using a HackerOne Challenge to augment and replace traditional pentests.

> We tried pentesting before and found it very expensive and practically useless. We paid many thousands of dollars and they only found a few bugs. The first week we launched HackerOne they found several high priority bugs we fixed immediately. Huge value at a fraction of the costs…
>
> **AMOS ELLISTON**
> *CTO, Flexport*

Pentests are a key part of any security apparatus, but the needs of today's rapid software development cycles, as well as the innovative methods of criminals, are far outpacing the results of periodic pentests. The solution is to use a large and diverse set of hackers to search for and report security vulnerabilities.

To learn more, see how HackerOne Challenge improves upon traditional pentests.

Cybersecurity Insurance: Reducing Risk with Hacker-Powered Security

A robust security program should be every organization's first line of defense. But security incidents are inevitable. Organizations are turning to cyber insurance to help with the recovery. Moody's Investors Service reported direct cyber insurance premiums grew to $2 billion last year, up 26 percent since 2015. The resulting damage to a brand and the cost of dealing with a cybersecurity issue can quickly reach tens or hundreds of millions of dollars.

Enter cybersecurity insurance, a relatively new vehicle for protecting organizations against the extreme costs resulting from a cybersecurity incident. In a recent interview, Deborah Chang, Vice President of Public Policy at HackerOne, said cybersecurity insurance is a new market that is making "a lot of noise."

But as with all things new, it's experiencing growing pains. Insurance companies do pay claims, the process gets murky as insurance underwriters may struggle to understand the technical aspects of a claim.

In a few very public cases, insurers refused to pay claims. The ongoing case of Mondelez International, the food company behind the Oreo and Ritz Cracker brands, is one prominent example. The company was impacted by the NotPetya attack in 2017, which ultimately cost them more than $100 million. Unfortunately, their insurer, Zurich Insurance, declined to reimburse the company, claiming the damage was the result of "war." Litigation is still ongoing.

In early 2019, several insurance firms offering cybersecurity insurance joined together to "collaborate to rate the efficacy of cybersecurity software and technology." The results of their rating would directly impact premiums paid, so those who use highly rated tools would see lower rates than those who don't. The proven impact of hacker-powered security should lead to higher ratings, thereby lowering premiums.

Still, even as this insurance might help defray the costs of a security incident, protecting systems and data to avoid an incident in the first place is still the most prudent approach. HackerOne is taking a proactive role in helping insurers better understand the security landscape and reduce the risks faced by their insured. These efforts include working closely with Travelers, as well as participating in educational efforts at Liberty Mutual Insurance, NetDiligence, Gallagher, and XL Catlin.

CUSTOMER SPOTLIGHT

“These new tactics empowered the community to earn an additional $250,000 in bounties from GitHub in 2018.”

GitHub

GitHub brings together the world’s largest community of developers to discover, share, and build better software. Their commitment to open source projects and the power of people makes its five-year partnership with the hacker community through HackerOne a natural fit.

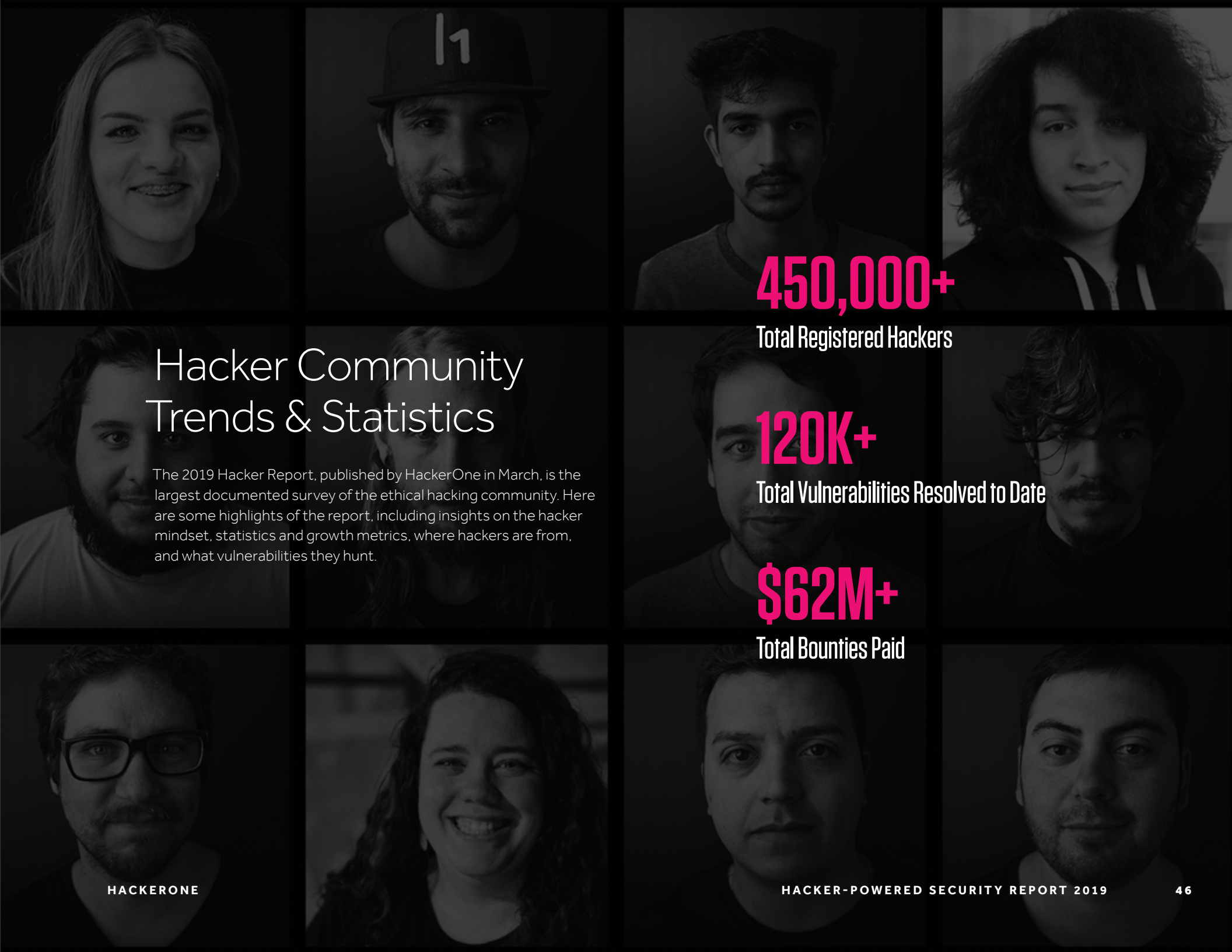
“GitHub launched our Security Bug Bounty program in 2014, allowing us to reward independent security researchers for their help in keeping GitHub users secure,” the company stated. “Over the past five years, we have been continuously impressed by the hard work and ingenuity of our researchers. Last year was no different and we were glad to pay out $165,000 to researchers from our public bug bounty program in 2018.”

GitHub continues to discover new and innovative ways to work with the close-knit community of hackers it has attracted through its long-standing program. Last year, GitHub added researcher grants, private bug bounty programs, and live hacking events to its existing bug bounty program, which allowed the company to reach a new crowd of hackers. These new tactics empowered the community to earn an additional $250,000 in bounties from GitHub in 2018.

INTRODUCING NEW WAYS TO KEEP YOUR CODE SECURE

GitHub wants to help close the gap between the hacker community and software engineers. Earlier this year they announced two new features including the addition of a SECURITY.md file to repositories and allowing people to collaborate on security advisories. HackerOne’s Policy Builder, allows you to generate a SECURITY.md file within minutes.

Hacker-powered security is more than just crowdsourcing vulnerability discovery. By taking the guesswork out of vulnerability reporting, GitHub is helping millions of engineers contribute more secure code.



Hacker Community Trends & Statistics

The 2019 Hacker Report, published by HackerOne in March, is the largest documented survey of the ethical hacking community. Here are some highlights of the report, including insights on the hacker mindset, statistics and growth metrics, where hackers are from, and what vulnerabilities they hunt.

450,000+
Total Registered Hackers

120K+
Total Vulnerabilities Resolved to Date

$62M+
Total Bounties Paid

Hacker Perceptions in America

In January 2019, HackerOne commissioned a survey, conducted online by The Harris Poll among over 2,000 U.S. adults to gauge their perception of hackers. The results, a portion of which are included below, are both encouraging and humbling. They represent part of an ongoing mission to redefine the term hacker in the likes of the Cambridge Dictionary, removing the unnecessary and incorrect association with criminality.

82%

of Americans believe hackers can help expose system weaknesses to improve security in future versions.

57%

Millennials (ages 18-34) are most likely to believe that hacking is a legitimate profession (57% vs. 31% of those ages 35+).

64%

of Americans think not all hackers act maliciously.

83%

More than 4 in 5 Americans believe hacking is an illegal activity.

Who are Hackers and Why Do They Hack?

Youthful, hungry for knowledge, and creative. Nine out of 10 hackers are under 35, while eight out of 10 are self-taught. More and more are coming from diverse industries outside of technology, allowing them to bring diverse skillsets and perspectives to bear on their bug hunts. They're also hacking more than 2018, with more than 40% spending 20-plus hours per week searching for vulnerabilities and making the internet safer for everyone.

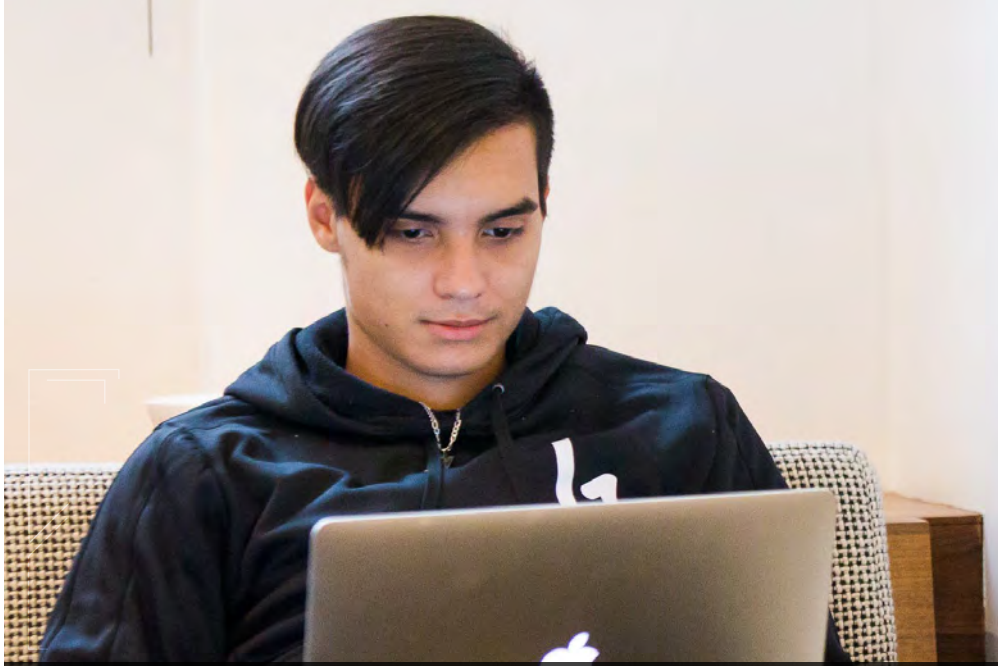
Hackers' motivation to join is not solely centered around bounties. Nearly three times as many hackers (41%) begin hacking to learn and contribute to their career and personal growth, and nearly as many hack to have fun (13%) as those who do it for the money (14%). With each new company and government agency joining HackerOne every day—such as the Hyatt Hotels, Airbnb, GitHub, Starbucks, HBO, U.S. Department of Defense, General Motors, Alibaba, Goldman Sachs, Toyota and more—comes curiosity and a genuine desire to help the internet become more secure (9%).

> "I think it's really important to hack in order to preserve the security of everything around us. There are so many applications we put our personal information into it and we just leave it out there. If it's not secure, what's to stop a malicious person from taking it?
>
> **@TEKNOGEEK**

The Economics of Bug Hunting

India, the United States, Russia, Pakistan, and the United Kingdom are the top locations where hackers reside, representing over 51% of all hackers in the HackerOne community. Six African countries had first-time hacker participation in 2018. Hackers from India and the U.S. alone account for 38% of the total community. That is a shift from 2018 when those two countries claimed 43%, demonstrating an exciting trend: increased global participation.

This globalization is in part due to the opportunities created by hacker-powered security. Top earners on HackerOne are making up to 40 times the median annual wage of a software engineer in their home countries, including HackerOne's first hacker to surpass $1 million in bounties. Some hackers have been awarded $100,000 for one critical vulnerability, and dozens of customers in the past year have hired hackers they met through their programs. Submitted bug reports, personal interactions, and public HackerOne profile activity contribute meaningfully to hiring decisions—a practice encouraged and championed within HackerOne.



HACKER COMMUNITY SPOTLIGHT

Santiago Lopez

From February through August of this year, six hackers made history as the first to earn more than $1,000,000 in bounty awards on HackerOne.

The first to reach the milestone was 19-year-old Argentinian Santiago Lopez, or @try_to_hack. Since joining HackerOne in 2015, Santiago has reported nearly 2,000 valid unique vulnerabilities to companies such as Verizon Media Company, Twitter, WordPress, Automattic, and HackerOne, as well as private programs. He consistently tops the HackerOne leaderboards, reaching the 91st percentile for signal and 84th percentile for impact, which ranks him 2nd overall on the platform with a reputation score of over 45,000. As a self-taught hacker, primarily using blogs and YouTube to expand his skills, Santiago shows us all that learning to hack is not reserved for the traditional classroom.

WHY DO YOU HACK?

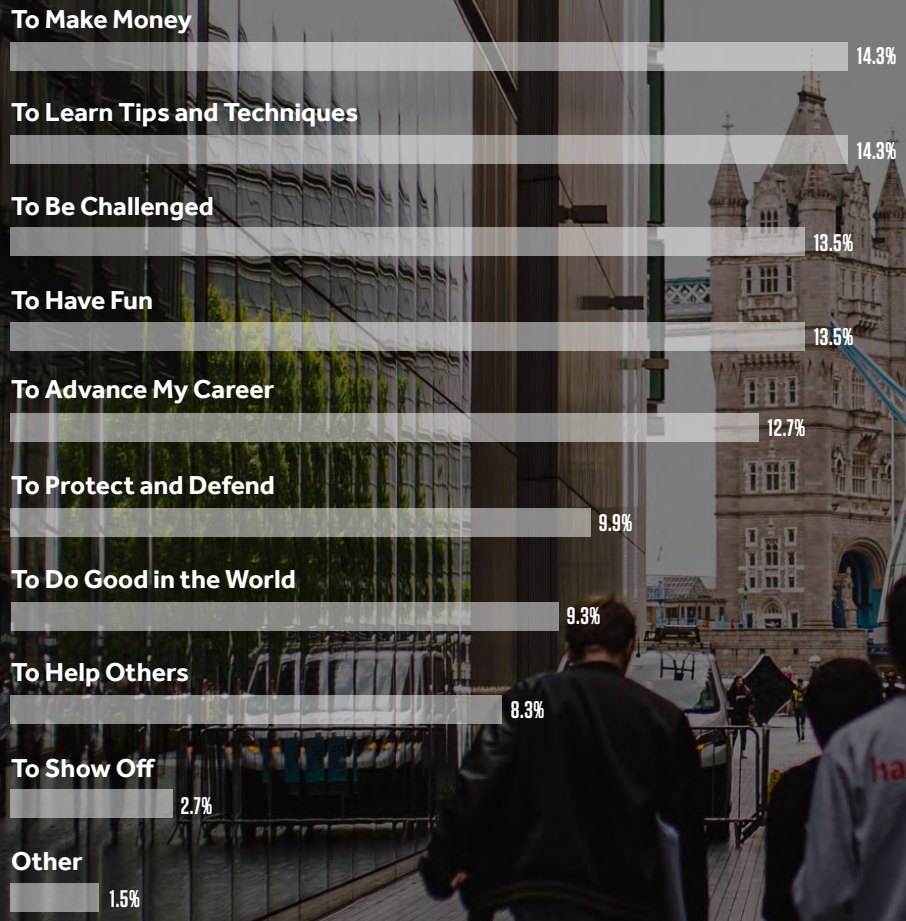


Figure 15

HACKERS' AGES

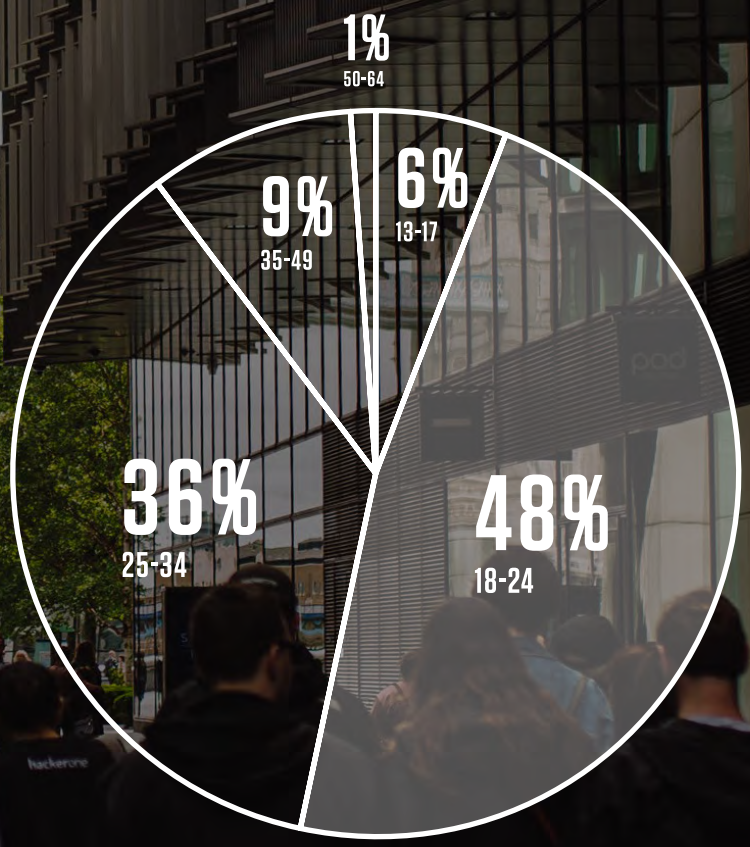


Figure 16

BUG BOUNTIES VS. SALARY

MULTIPLIER OF MEDIAN ANNUAL EARNINGS FOR TOP HACKER

40.6x
ARGENTINA

24.5x
THAILAND

24.2x
EGYPT

17.6x
INDIA

6.7x
HONG KONG

6.4x	UNITED STATES OF AMERICA
6.3x	SWEDEN
6.2x	CHINA
6.2x	ALGERIA
4.8x	CANADA
3.9x	PAKISTAN
3.8x	MOROCCO
3.5x	LATVIA
3.1x	BELGIUM
3.0x	PHILIPPINES
3.0x	AUSTRALIA
2.9x	NEW ZEALAND
2.9x	GERMANY
2.9x	PORTUGAL
2.7x	HUNGARY
2.5x	ROMANIA
2.5x	CHILE
2.5x	ETHIOPIA
2.4x	INDONESIA
2.2x	NETHERLANDS

Figure 17: *Median annual wage of a security engineer was derived from PayScale for each region. The multiplier is the top bounty earnings divided by the median annual wage of a software engineer.*

Hacker Education

Cybersecurity skills are in high demand. New research by Cybersecurity Ventures predicts 3.5 million unfilled cybersecurity positions by 2021. The hacker community is growing, but just 6% have completed a formal class or certification on hacking and 81% say they learned their craft mostly through blogs and self-directed educational materials and publicly disclosed reports. To train future cybersecurity leaders, the broader security community needs to invest in education. HackerOne is committed to preparing students for success as ethical hackers through programs such as Hacker101.

The Hacktivity feed remains a resource for hackers to learn from their peers. Of note, in total, over 6,200 reports have been disclosed on HackerOne's Hacktivity.

hacker101

Hacker101 is a free web security training series for the next generation of ethical hackers. Whether you're a programmer with an interest in bug bounties or a seasoned security professional, Hacker101 has something to teach you. The video library, which we add to each month, covers basics like The Web in Depth, common and emerging vulnerabilities types, and how to find them, as well as advanced topics like mobile and native code hacking.

Hacker101 CTF (Capture The Flag) is a series of free hacking games based on real-world environments that challenge learners to hack in and find the flags. Experienced and aspiring hackers can put their skills into practice with levels inspired by the real world security vulnerabilities. Flags are placed in various locations such as a file, a database, or source code. To complete the CTF, learners hunt down all the flags using the skills from the Hacker101 videos. With new levels added every month, there's always a new challenge waiting. Should students get stuck, the 6,500+ members of our online Discord discussion server are available 24/7. Organizations looking for security help recognize the value of Hacker101 training. Finding flags in a CTF allows hackers to directly earn invitations to private bug bounty programs on HackerOne.

To celebrate $50M in bounties paid to hackers on the HackerOne platform as of April 2019, we announced our most advanced CTF ever which presented challenges spanning from mobile, crypto, and the web. Hackers had to first hunt down the "HackerOne Thermostat" app, break into the backend, and find their way into the thermostat itself to finally get into the accounting server to steal the flag. Hundreds of hackers participated, but only a select few were able to make it all the way to the end. This was the first time we created a dedicated space, a channel on our Discord server, for folks to chat about one of our big CTFs. It was thrilling to watch thousands of messages fly back and forth, especially as hackers hit one of our favorite red herrings, a fake SQL parser. The results really speak for themselves; we received so many outstanding submissions and saw more creativity than ever before.

In 2018 Hacker education got another boost with the introduction of Hackboxes: Sandbox environments of disclosed vulnerability reports on HackerOne's Hacktivity where learners can test their skills in real-world simulated bugs. The 5 Hackbox environments were launched with the help of HackEDU and are available for anyone to test their hacking skills and see if they can replicate the same bug that was discovered.

Live Hacking Events

Our tagline, "Together We Hit Harder" is born of the belief that when hackers and security teams are connected, security improves. Nothing captures that truth better than live hacking events (LHE).

Live hacking is a unique type of bug bounty engagement in which hackers from all over the globe fly in to participate in an in-person, timeboxed testing period focusing on a targeted set of assets. This traditionally includes two weeks leading up to the event culminating in 2-3 days in a particular city. During those several days, we bring the programs' security teams and hackers together for social activities, sightseeing, knowledge-sharing, and of course, lots of hacking Special scopes are released for more compelling testing, companies are encouraged to provide metadata or unique feature access for additional research, cash bonuses and bounties are offered, and there's a leaderboard for the event with awards for the top hackers for best bug, best signal, highest reputation gain, and the best hacker of the event (Most Valuable Hacker). We also host hacking workshops for student groups, structured hacking mentorship sessions and job recruiting workshops.

The first live hacking event was set up by Frans Rosen and Justin Calmus in 2015. They invited friends that were in town attending DEFCON to a suite at the MGM Grand in Las Vegas for eight solid hours of hacking. You can read more on this in Frans' BountyCon 2019 keynote. HackerOne's first live hacking event, h1-702, was in Las Vegas in August 2016 during DEF CON and spanned three days, paying out over $150K to a group of about 30 hackers. Live hacking events have come a long way since then, improving the structure and experience for top hackers and customers alike.

LIVE HACKING EVENTS

10
DIFFERENT CITIES AROUND THE WORLD

30.2%
AVERAGE HIGH + CRITICAL SEVERITY REPORTS

13
CUSTOMERS

36
DAYS OF HACKING

18
EVENTS

$2,000,000
HIGHEST AMOUNT PAID OUT AT SINGLE EVENT (H1-702, 2019)

Mentorship Program and Community Days

Community days focused on diversity and inclusion have become an ingrained part of HackerOne's traveling live hacking events. They bring together local cybersecurity focused organizations like preparatory schools, groups like Cyber Patriots, Hack the Hood, Black Girls Code, and WiSP together with top hackers and educators. These in-person events give aspiring hackers a chance to learn Hacker101 content from seasoned hackers. Each community day starts with seasoned hackers sharing their journey with bug hunting. Then attendees are led through a hands-on educational session with capture-the-flag challenges, building on the Hacker101 curriculum. All attendees are shown how to find their first bug or advance to the next level in their hacking career. Community day attendees experience the full live hacking event, plus they receive advanced instruction and guided mentorship.

Find out more HackerOne community days and live hacking events and how to participate.

Security@ Conference

In October 2018, HackerOne hosted the largest-ever hacker-powered security conference, The second annual Security@ Conference in San Francisco. The one-day event brought together more than 350 security leaders, influencers, and hackers from around the world to discuss lessons, learnings, and insights of those who are leading us into the modern era of cybersecurity.

Speakers included hackers such as Keren Elazari, Jack Cable, Frans Rosen, cache-money and Johnny Nipper, as well as Reina Staley from Defense Digital Service, Verizon Media CISO Chris Nims, Leonard Bailey from the Department of Justice, Yelp Director of Engineering Vivek Raman, Kate Conger from The New York Times, cybersecurity reporter Patrick Howell O'Neill, technology reporter Bree Fowler, and Sumo Logic CSO George Gerchow, among others.

If you're wondering what Security@ is all about, look no further than the name. The name "Security@" refers to the "security@[organization].com" alias, which many businesses use to allow researchers to submit bug reports. It pays homage to the people, stories, and creativity on both sides of that email address.

Security@ attracts trailblazers from across the industry: hackers, influencers, experts, and innovators from some of the world's most advanced security teams. On October 15, 2019, for the third year in a row, the security community will gather at Security@ to share the latest lessons and insights from the hacker front lines.

To join us at Security@ 2019, register now.

BRINGING THE COMMUNITY TOGETHER FOR GLOBAL LIVE EVENTS

Figure 18: *HackerOne holds live hacking events around the world to bring hackers and security teams together, in person, to build stronger relationships, learn from each other, and, most importantly, quickly resolve security vulnerabilities.*

History of Hacker-Powered Security

A timeline of defining events related to vulnerability disclosure policies, bug bounties, security research, and hackers.

1983

Hunter & Ready, Inc. announces a "bug" bounty program for their products.

1995

Netscape launched the first "modern-day" bug bounty program, offering monetary rewards for Netscape Navigator 2.0 Beta.

2004

August: Mozilla Foundation started offering bug bounties up to $500 for critical vulnerabilities.

2007

The first PWN2OWN contest kicked off.

1983: The first known "bug" bounty program that paved the way for today's industry is launched by operating system company Hunter & Ready, Inc.

1988: In response to the first major computer virus, the Computer Emergency Response Team (CERT) coordination center is created to research software vulnerabilities.

1995: Netscape launches the first modern-day bug bounty program, offering monetary rewards for Netscape Navigator 2.0 Beta.

1998 | **May:** Seven members of Boston-based hacker think tank "L0pht" appeared before a Senate committee and bluntly stated that networks of computers and software were terribly insecure.

1999: Nomad Mobile Research Center (NMRC) publishes a bug disclosure policy stating their intent to verify problems and contact vendors with technical details.

2002 | **February:** Chris Wysopal and Steve Christey of the Internet Engineering Task Force publish the Responsible Vulnerability Disclosure Process.

2002 | **August:** IDefense's Vulnerability Contributor Program launches with rewards to researchers who find vulnerabilities in software systems.

2002 | **August:** Open Sourced Vulnerability Database (OSVDB) is launched to provide technical information on vulnerabilities.

2004 | **August:** Mozilla Foundation starts offering bug bounties up to $500 for critical vulnerabilities found in Firefox and other Mozilla software.

2005 | **July:** Zero Day Initiative launches to help connect security researchers with vendors and encourage the responsible reporting of zero-day vulnerabilities through financial incentives.

2007: The first PWN2OWN contest kicks off, igniting a competition to exploit Mac OSX across a limited time frame.

2010

Google announces a bug bounty program for web applications.

2011

July: Facebook announces a bug bounty program.

2012

HackerOne is founded with the mission to empower the world to build safer internet.

2013

November: Microsoft and Facebook sponsor the creation of Internet Bug Bounty (IBB).

2009 | **March:** Alex Sotirov, Dino Dai Zovi, and Charlie Miller petition for "no more free bugs" at the CanSecWest conference.

2010: Google announces a bug bounty program for web applications, Mozilla expands its program to include web properties, and Microsoft announces their Coordinated Vulnerability Disclosure Policy.

2011 | **April:** Microsoft implements a new company policy requiring all employees to follow a detailed set of procedures when reporting security vulnerabilities in third-party products.

2011 | **July:** Facebook announces a bug bounty program with a $500 minimum reward for valid bugs.

2012: HackerOne is founded with the mission to empower the world to build a safer internet.

2013 | **March:** The Government of the Netherlands publishes their Guideline for responsible disclosure of IT vulnerabilities.

2013 | **October:** Microsoft offers its first bug bounty to identify bugs in Internet Explorer.

2013 | **November:** Facebook and Microsoft sponsor the creation of the Internet Bug Bounty (IBB) program for core internet infrastructure and free open source software.

2014 | **January:** Microsoft helps draft ISO/IEC 29147:2014, which provides guidelines for the disclosure of potential vulnerabilities in products and online services.

2014 | **April:** HackerOne launches Hacktivity, showcasing public vulnerability coordination activity occurring on the HackerOne platform.

2014 | **July:** Google creates Project Zero, a team of top security researchers working full-time to identify zero-day vulnerabilities in any software.

2016

April: Hack the Pentagon pilot bug bounty program launches.

2016

May: Manifesto on coordinated cybersecurity disclosure signed by 29 companies.

2016

November: The U.S. Department of Defense kicks off the first government VDP.

2016

December: The NTIA Safety Working Group published v1.1 of Coordinated Vulnerability Disclosure Template.

2015 | **August:** Oracle's security chief, Mary Ann Davidson, publishes a rambling missive against the security research industry.

2015 | **November:** HackerOne launches Disclosure Assistance to help hackers report vulnerabilities safely to organizations without public disclosure programs.

2016 | **January:** European Union Agency for Network and Information Security (ENISA) publishes "Good Practice Guide on Vulnerability Disclosure" to propose recommendations for vulnerability disclosure.

2016 | **April:** First Federal bug bounty program, Hack the Pentagon launches.

2016 | **May:** Global Forum on Cyber Expertise announces that 29 organizations signed the "Coordinated Vulnerability Disclosure Manifesto" to showcase their public vulnerability reporting mechanisms.

2016 | **August:** HackerOne kicks off its first live hacking event in Las Vegas, H1-702, paying out over $150K in bounties in just 3 days.

2016 | **November:** The U.S. Department of Defense kicks off the first government VDP.

2016 | **December:** National Telecommunications and Information Administration (NTIA) Safety Working Group publishes v1.1 of "Coordinated Vulnerability Disclosure Template" as a guide for companies on security researcher disclosure best practices and policies.

2016 | **December:** Food and Drug Administration issues "Postmarket Management of Cybersecurity in Medical Devices" to inform industry and FDA staff of the Agency's recommendations for proactively managing cybersecurity vulnerabilities.

2017 | **February:** Federal Trade Commission provides comments on the NTIA's "Coordinated Vulnerability Disclosure Template," stating that "the template could be a useful tool for any company providing software-based products and services to consumers."

2017

August: The CERT Guide to Coordinated Vulnerability Disclosure is published.

2017

October: US Deputy Attorney General Rod J. Rosenstein recommends all companies should consider promulgating a vulnerability disclosure policy.

2018

February: HackerOne and others invited to testify in front of the U.S. Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security.

2018

April: H.R. 5433: Hack Your State Department Act proposed by Representative Ted Liu.

2017 | **May:** Hack the DHS, a bill to establish a bug bounty pilot program within the Department of Homeland Security is proposed, and later in 2018 passes the U.S. Senate by unanimous vote.

2017 | **July:** U.S. Department of Justice publishes A Framework for a Vulnerability Disclosure Program for Online Systems.

2017 | **August:** Carnegie Mellon University's Software Engineering Institute publishes "The CERT® Guide to Coordinated Vulnerability Disclosure" to describe best practices for when vulnerabilities are discovered.

2017 | **August:** UC Berkeley class CS 194-138/294-138 opens to undergraduate and graduate level engineering students with a cybersecurity curriculum utilizing bug bounty programs in coursework.

2017 | **August:** U.S. Senators Cory Gardner (R-CO) and Mark R. Warner (D-VA), co-chairs of the Senate Cybersecurity Caucus, along with Sens. Ron Wyden (D-WA) and Steve Daines (R-MT), introduce bipartisan legislation to improve the cybersecurity of Internet of Things (IoT) devices.

2017 | **October:** In remarks delivered at the Global Cybersecurity Summit, Deputy Attorney General Rod J. Rosenstein says "All companies should consider promulgating a vulnerability disclosure policy."

2018 | **February:** HackerOne and others testify before the U.S. Senate on the benefits and nature of hacker-powered security. Senators express their support for this vital form of cybersecurity.

2018 | **April:** Hack Your State Department Act is proposes and would require the Secretary of State to design and establish a VDP.

2018 | **April:** Facebook announces their Data Abuse Bounty, offering rewards for reports of data abuse.

2018 | **May:** Goldman Sachs becomes the first investment bank to launch a public VDP.

2018 | **June:** U.S. Representatives Mike Quigley (R-IL) and John Katko (R-NY) introduces "Hack the Election" or the Prevent Election Hacking Act of 2018 to help combat the threat of election hacking in part by creating a bug bounty program.

2018

October: Second annual dedicated hacker-powered security conference, Security@ 2018, takes place in San Francisco.

2019

January: 19-year-old Santiago Lopez becomes the first bug bounty hacker to surpass $1,000,000 in bounty awards.

2019

March: HackerOne hacker community surpasses 300,000 with more than 600 hackers registering any given day.

2019

April: HackerOne exceeds $50,000,000 in bounties paid out to hackers.

2018 | **September:** U.S. General Services Administration, the first civilian agency to run a bug bounty program, selects HackerOne as TTS bug bounty partner.

2018 | **October:** U.S. Department of Defense awards HackerOne third hack the pentagon "crowdsourced security" contract.

2018 | **October:** Second annual dedicated hacker-powered security conference, Security@ 2018, takes place in San Francisco.

2019 | **January:** Hyatt becomes first global hotel hospitality company to launch a public bug bounty program.

2019 | **January:** 19-year-old Santiago Lopez becomes the first bug bounty hacker to surpass $1,000,000 in bounty awards.

2019 | **February:** HackerOne opens regional office in Singapore.

2019 | **March:** HackerOne hacker community surpasses 300,000 with more than 600 hackers registering any given day.

2019 | **March:** U.S. Presidential candidate Beto O'Rourke identified as a member of the oldest computer hacking group in U.S. history.

2019 | **April:** HackerOne exceeds $50,000,000 in bounties paid out to hackers.

2019 | **May:** Economic impact study finds crowd sourced penetration testing can deliver 115% return on investment over three years.

2019 | **June:** HackerOne opens regional office in France.

2019 | **June:** U.S. Senators introduces the Hack Your State Department Act that would require a Vulnerability Disclosure Process and bug bounty program.

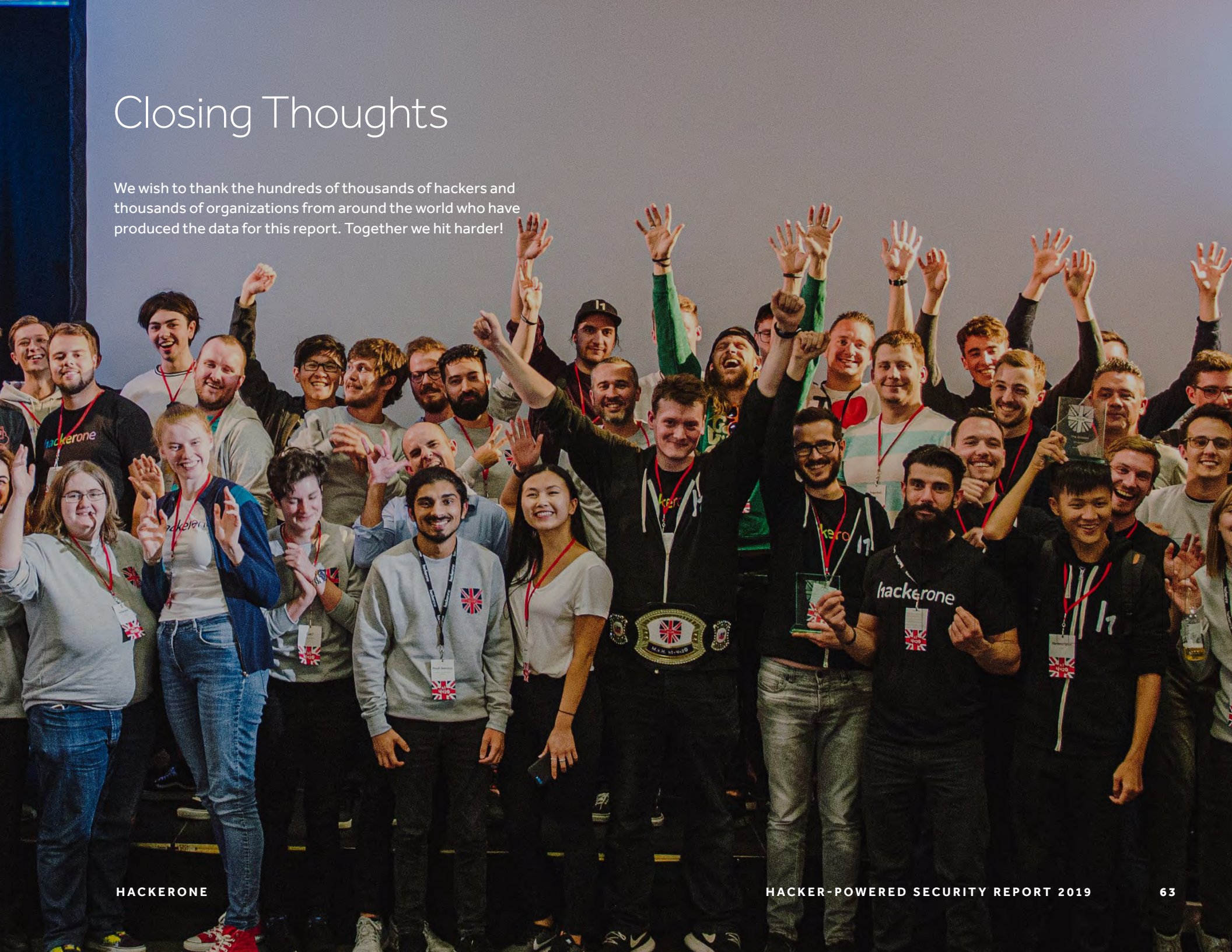
2019 | **August:** Capital One thanks hacker for reporting unauthorized access to their responsible disclosure program.

2019 | **August:** Apple's bug bounty program ups its max payout to $1,000,000.

2019 | **August:** HackerOne sets bug bounty record awarding hackers $2,000,000 during a single live hacking event.

Closing Thoughts

We wish to thank the hundreds of thousands of hackers and thousands of organizations from around the world who have produced the data for this report. Together we hit harder!



Methodology & Source

Findings in this report were collected from the HackerOne platform using HackerOne's proprietary data based on over 1,400 collective bug bounty and vulnerability disclosure programs.

FORBES GLOBAL 2000 VULNERABILITY DISCLOSURE RESEARCH

Our research team searched the Internet looking for ways a friendly hacker could contact these 2,000 companies to disclose a vulnerability. The team looked for web pages detailing vulnerability disclosure programs as well as email addresses or any direction that would help a researcher disclose a bug. If they could not find a way for researchers to contact the company to disclose a potential security vulnerability, they were classified as not having known disclosure program.

Any companies that do have programs but are not listed as having one in the Disclosure Directory are encouraged to update their profile in the Disclosure Directory on their company's page. See ISO 29147 for additional guidance or contact us.

THE 2019 HACKER REPORT

Data collected from HackerOne Platform, survey data in December 2018, and survey of U.S. adults in January 2019 totaling over 3,667 respondents from over 100 countries and territories. The HackerOne platform individuals surveyed have each successfully reported one or more valid security vulnerabilities on HackerOne, as indicated by the organization that received the vulnerability report. Additional findings were collected from the HackerOne platform using HackerOne's proprietary data based on over 1,400 collective bug bounty and vulnerability disclosure programs.

About HackerOne

HackerOne is the #1 hacker-powered pentest and bug bounty platform, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. The U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Microsoft, MINDEF Singapore, HBO, Intel, IBM, Qualcomm, Starbucks, Dropbox, Intel, the CERT Coordination Center and over 1,400 other organizations have partnered with HackerOne to find over 120,000 vulnerabilities and award more than $62M in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York, France, the Netherlands, and Singapore.

Trusted By

More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative.