hackerone

Worldwide Security Coverage for Unlimited Reach

HackerOne's International Community of White-Hat Hackers Protects the Applications, Data, and Users of Organizations Far and Wide

Borders Don't Deter Cybercriminals

The Internet is an amazing human innovation. It enables your organization to give instant access to information to anyone, anywhere in the world. You have rules for displaying that information. Your region or country has rules as well, as does the region of those accessing your information.

But cybercriminals aren't bound by borders. The Internet gives them access to tools, systems, and data across the globe, and they're not afraid to use their methods wherever they can.

Cybercrime cost the world nearly US$600 billion in direct losses in 2017 alone. Countries with the largest populations—China, Brazil, the United States, and India—bear the financial brunt of those crimes. However, countries like France, the United Kingdom, Italy, Sweden, Germany, Japan, Spain, Australia, the Netherlands, and the United Arab Emirates were each hit with more than US$1 billion in cybercrime in 2017. And the total cost of damages due to cybercrime, from stolen money to lost productivity to brand impact, is expected to hit US$6 trillion by 2021.

But just as those impacted by cybercrime hail from all over the world, the number of countries from which cybercrime originates continues to grow. Today's cybercrime "hotspots" include Russia, Ukraine, Romania, Nigeria, Brazil, China, and the United States.

A Global Community to Counter a Global Challenge

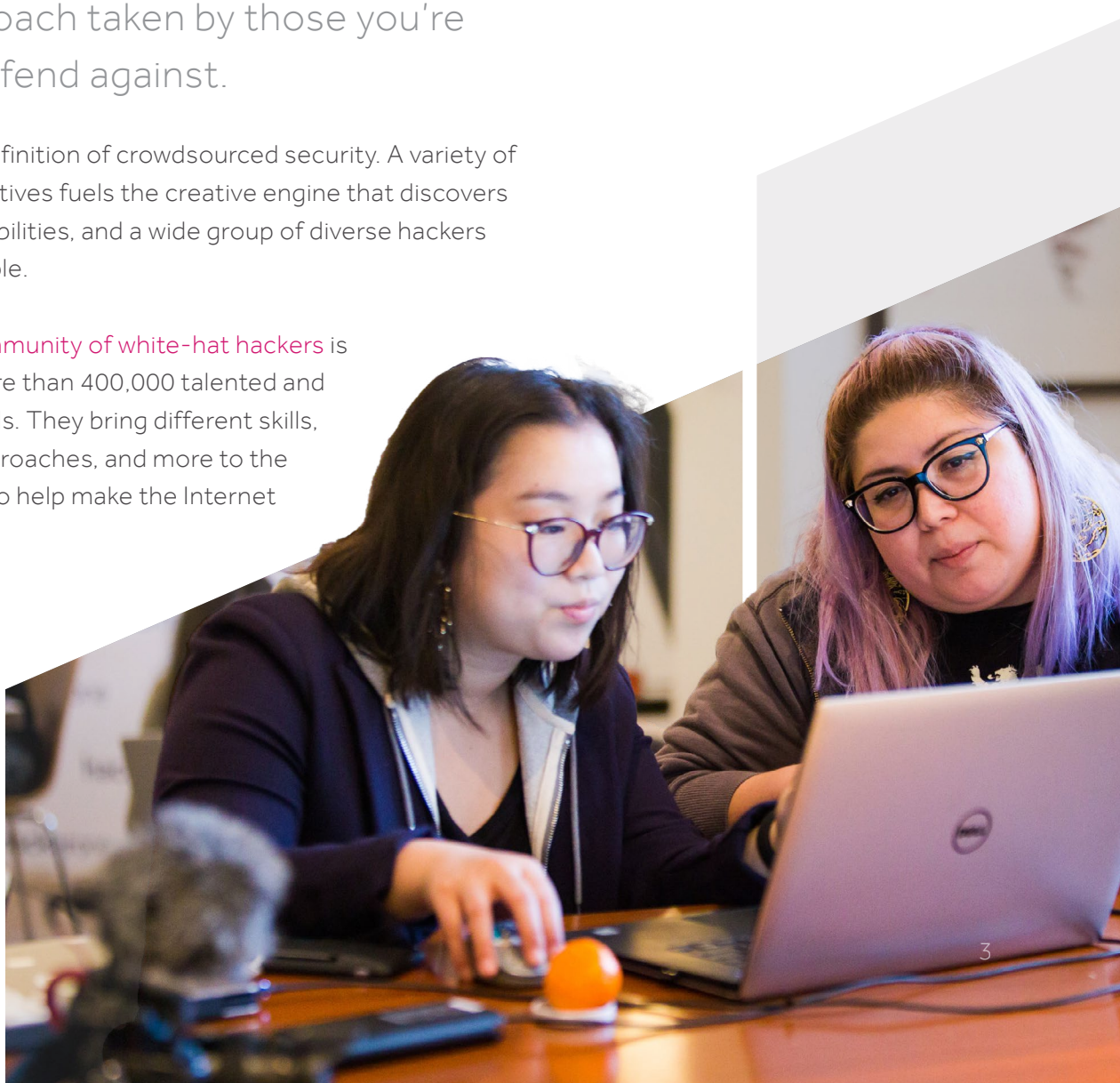
When your adversaries are many, diverse, and dispersed across the globe, it's unreasonable to assume a small, regionally-limited team is equipped to handle every threat. Criminals are creative, have broad and varied perspectives, and aren't limited by rules, regulations, laws, or even budgets. Limiting your security resources is counter to the approach taken by those you're trying to defend against.

"By opening up these types of challenges to more countries and individuals, we get a wide range of talent and experience we would normally not have access to in order to harden our networks."

— CAPTAIN JAMES "JT" THOMAS, AIR FORCE DIGITAL SERVICE

Diversity is the definition of crowdsourced security. A variety of skills and perspectives fuels the creative engine that discovers impactful vulnerabilities, and a wide group of diverse hackers makes this possible.

HackerOne's community of white-hat hackers is comprised of more than 400,000 talented and creative individuals. They bring different skills, perspectives, approaches, and more to the table, every day, to help make the Internet a safer place.

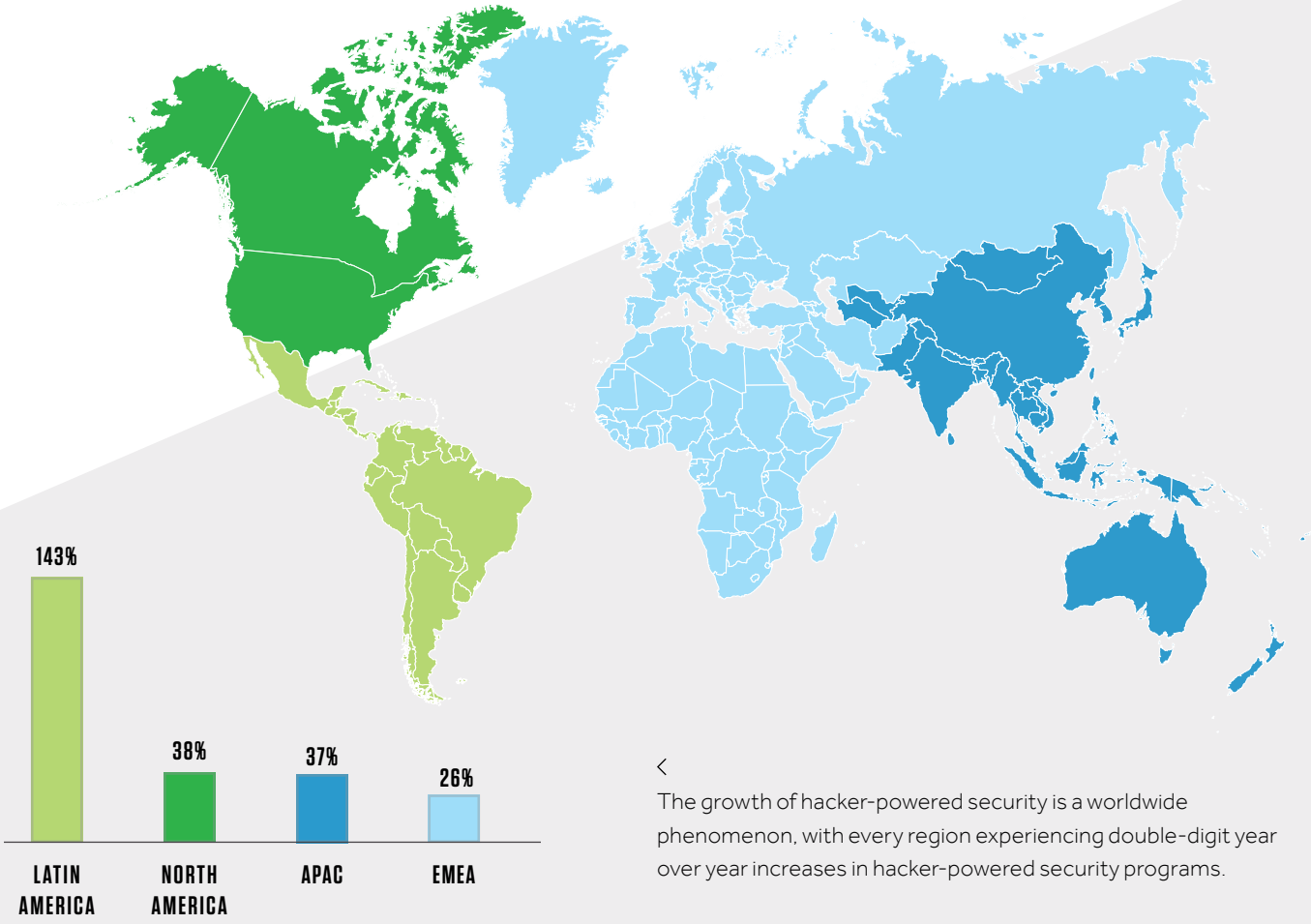


The HackerOne community is decidedly global. Countries as diverse as Iceland, Ghana, Slovakia, Aruba, and Ecuador have hackers with as much determination, skill, and success as those from the more popular hacker homes of India, the United States, Russia, Pakistan, and the United Kingdom. HackerOne also has deep roots in Europe: the company was founded in the Netherlands and nearly 40% of the HackerOne community resides in EMEA countries.

Hacker globalization is sparked by the same mechanisms driving the growth of the Internet itself, including near-ubiquitous access to online opportunities. Smart, creative hackers can access lucrative and challenging cybersecurity opportunities from anywhere in the world—all they need is an Internet connection.

HackerOne makes it easy for organizations and governments anywhere in the world to work directly with these hackers to find vulnerabilities, with no limits.

Program Origination Growth in Respective Regions since 2016

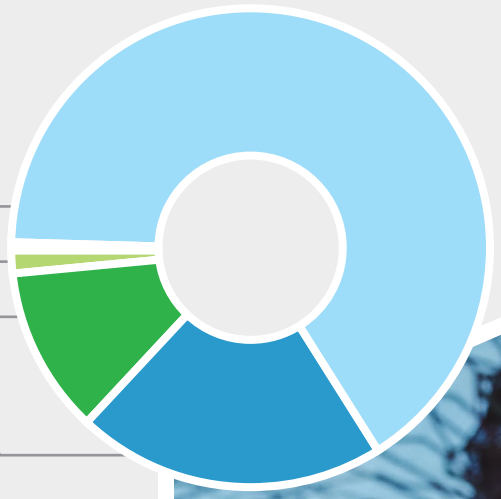


The growth of hacker-powered security is a worldwide phenomenon, with every region experiencing double-digit year over year increases in hacker-powered security programs.

Hackers and Bounties by Sign-in Region

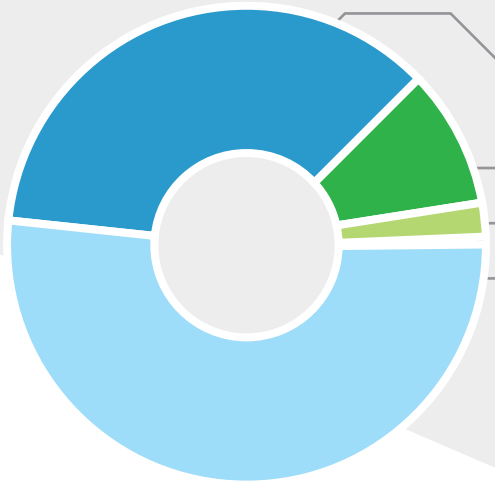
Smart, talented, and skilled hackers hail from all corners of the globe, and those earning bounty awards are as likely to be from Europe as from any other region.

BOUNTIES AWARDED TO HACKERS BY SIGN-IN REGION



EMEA	$3,294,533
LATIN AMERICA	$66,283
NORTH AMERICA	$565,067
APAC	$1,041,258

HACKERS BY SIGN-IN REGION



APAC	3,856
NORTH AMERICA	1,011
LATIN AMERICA	219
EMEA	5,522

To better support a global community of hackers and a growing global network of organizations using hacker-powered security, HackerOne continues to build a global presence. We are headquartered in San Francisco, have teams to support customers and hackers in Europe and Asia, and have offices in London, New York City, Singapore, and the Netherlands.

Singapore's Government Technology Agency (GovTech) and Cyber Security Agency of Singapore (CSA) used hacker-powered security as part of the Singapore Government's ongoing initiative to build a secure and resilient Smart Nation. During a three week HackerOne Challenge, a global team of hackers searched for vulnerabilities across the Singapore Government's digital assets. Hackers ultimately earned US$11,750 for reporting 26 valid security weaknesses.

Regulators are Encouraging a Borderless Approach to Cybersecurity

With the European Union's installation of the General Data Protection Regulation (GDPR), the approach to online accountability took a major leap towards a borderless approach. GDPR takes aim at every business, organization, or government agency that collects information on European Union (EU) citizens. Since the Internet provides global access, and EU citizens are free to visit websites that originate in any country, nearly every online entity was forced to change how it manages customer data and security.

GDPR also prompted organizations to add hacker-powered security to their efforts given the regulation's provisions for regular testing and limiting access to personal data. A global hacker community can form the basis of a continuous, 24x7 force to test code, search for vulnerabilities, and report bugs. This further provides a greater ability to find vulnerabilities on your own terms and via a process you control so there's no need to disclose it per GDPR.

The Centre for European Policy Studies (CEPS), an EU think tank, also provided guidelines for software vulnerability disclosure (SVD) across the European Union. Their 2018 report called upon the European Commission and the member states to draft a continent-wide framework and accompanying national legislation to provide legal clarity around software vulnerability discovery and disclosure.

HackerOne Response is a dedicated product available to help organizations quickly implement a compliant, proven methodology with minimal deployment or ongoing management costs. It's a simple way to streamline disclosure for those new to vulnerability disclosure or those experiencing related cost, management, or other challenges.

HOW VULNERABILITY DISCLOSURE AND HACKER-POWERED SECURITY SUPPORT GDPR COMPLIANCE

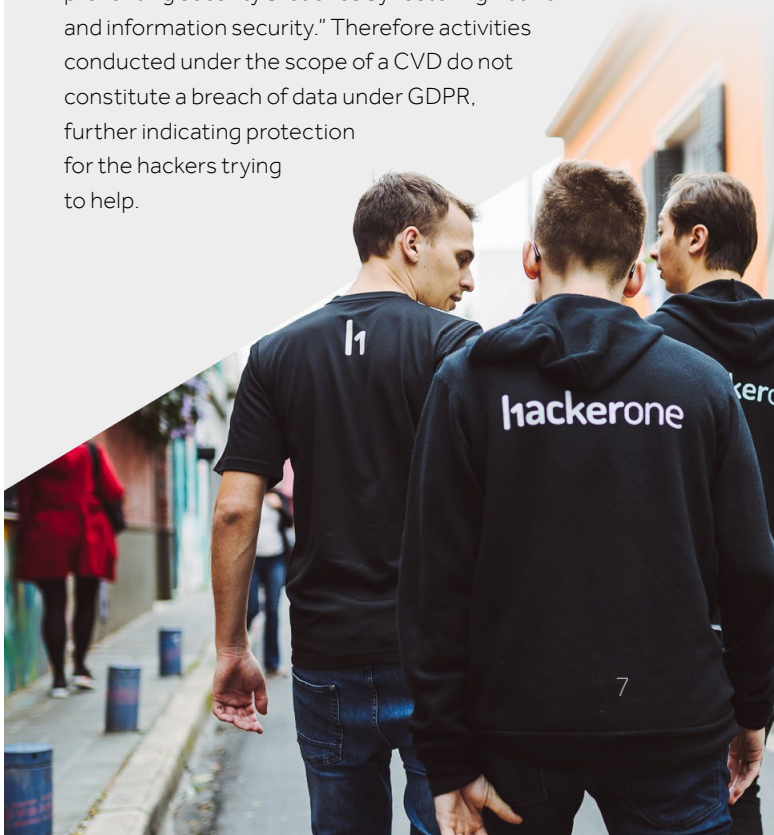
The Centre for European Policy Studies (CEPS) initiated a task force to define guidelines around vulnerability disclosure across the European Union. In their final report, they stressed GDPR's relevance to coordinated vulnerability disclosure (CVD), going so far as to say "irresponsible handling of vulnerabilities could lead to personal data breaches falling within the scope of GDPR, (therefore) CVD should be viewed as one of the necessary tools to mitigate the relevant risks."

In short, irresponsible handling of vulnerabilities is a violation of GDPR and CVD can help avoid liability under the regulation. CEPS also says that the mere presence of a CVD and the timely handling of vulnerabilities "may reduce the risk of incurring fines arising from possible personal data breaches." Read another way, the absence of a CVD could be seen as not only irresponsible, but worthy of penalties.

CEPS further voiced support for hacker-powered security, stressing that, under GDPR's concerns over processing of personal data, CVDs should be considered "of a legitimate interest of the controller in preventing security breaches by fostering network and information security." Therefore activities conducted under the scope of a CVD do not constitute a breach of data under GDPR, further indicating protection for the hackers trying to help.

These and other initiatives point to the leadership of the EU and member countries on issues of cybersecurity. But the focus on security is growing globally, as is the clear embrace of hacker-powered security.

To help meet stringent regulatory or internal requirements, HackerOne Challenge and private HackerOne Bounty also provide controls so organizations can limit program participation to hackers from specific countries or regions.

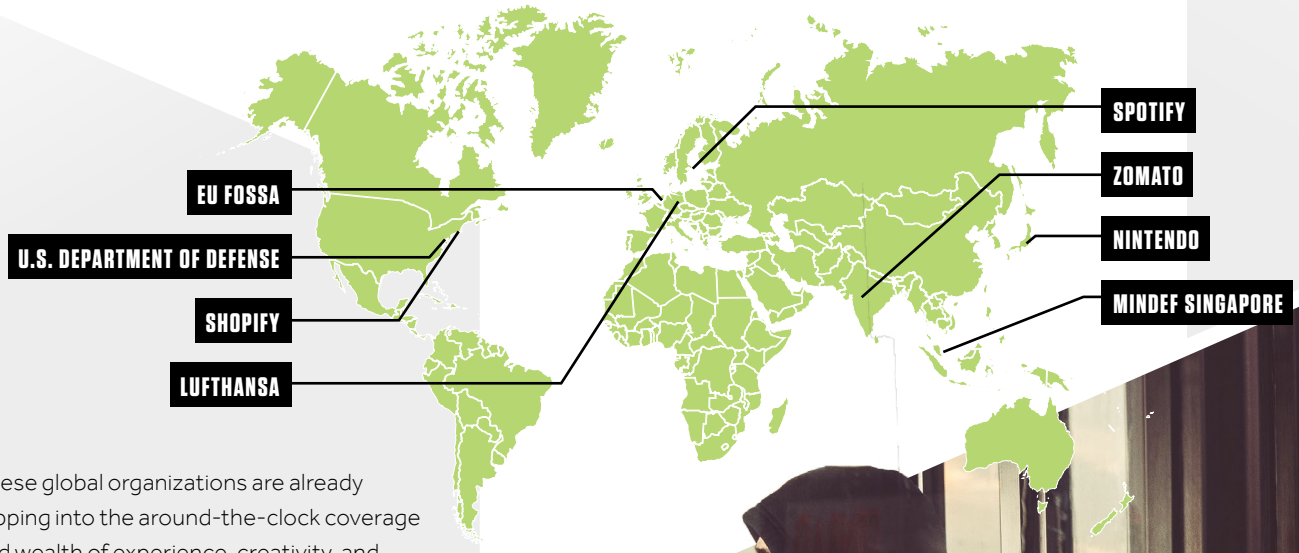


Global Security Needs Global Experience

The U.S. Department of Defense, arguably the most security-aware organization on the planet, has used the HackerOne platform to resolve more than 5,000 vulnerabilities in less than two years. Programs like Hack the Pentagon, Hack the Army, and Hack the Air Force have helped the Department of Defense secure and protect sensitive data and systems with the help of HackerOne's community of diverse, creative, and expert hackers.

But other organizations with similar levels of security awareness have also taken steps to incorporate hacker-powered security into their efforts. The European Commission, for example, selected HackerOne as the platform for their first ever bug bounty program. Singapore's Ministry of Defence (MINDEF) also works with HackerOne's global community to identify vulnerabilities in its public-facing systems.

Global Organizations Trusting Hacker Powered Security



These global organizations are already tapping into the around-the-clock coverage and wealth of experience, creativity, and approaches available through a global community of white-hat hackers.

EU-FOSSA Project

The European Commission's first ever bug bounty program was developed through the EU-Free and Open Source Software Auditing (EU-FOSSA) project, which aims to help EU institutions better protect their critical software. EU-FOSSA was created in the aftermath of the Heartbleed incident, which highlighted the presence of vulnerabilities in software widely used across the Commission.

The EU-FOSSA project, now in its second iteration, has received over 400 vulnerability reports and awarded nearly €100,000in bounties.

Singapore MINDEF

Singapore's Ministry of Defence ran the country's first crowd-sourced security initiative, which was also the first program of its kind run by a government agency in Asia. The program, which ran for just 3 weeks, attracted more than 260 hackers located in countries as diverse as Canada, Egypt, India, Ireland, Pakistan, Romania, Russia, Singapore, Sweden, and the United States. The total bounty payout was US$14,750 for 35 validated reports.

"There's no other existing process, including paying a company to test our systems, which would have allowed us to discover this number of previously unknown vulnerabilities so quickly, so effectively and at this cost," said David Koh, Mindef's defence cyber chief.

GOVERNMENT AGENCIES USE HACKERONE

Government organizations from around the world recognize the benefits and value of using white-hat hackers to enhance their security posture. From defense to general services to desktop applications, HackerOne and our community of global hackers are keeping public data and systems safe. To learn more, download this ebook today.

DOWNLOAD NOW

HACK THE PENTAGON

HACKERONE CHALLENGE

1,400+
HACKERS REGISTERED

13 minutes
FIRST REPORT

$75,000
BOUNTIES PAID

138
VALID REPORTS

U.S. DEPARTMENT OF DEFENSE

HACKERONE RESPONSE

650+
HACKERS PARTICIPATING

3,000+
VULNERABILITIES RESOLVED

HACK THE ARMY

HACKERONE CHALLENGE

371
HACKERS PARTICIPATING

5 minutes
FIRST REPORT

$100,000
BOUNTIES PAID

118
VALID REPORTS

HACK THE AIR FORCE

HACKERONE CHALLENGE

275+
HACKERS PARTICIPATING
with 30 from outside U.S.

1 minute
FIRST REPORT

$233,883
BOUNTIES PAID
($130,000 + $103,883)

313
VALID REPORTS
(207 + 106)

U.S. DEPARTMENT OF DEFENSE USES THE GLOBAL HACKER COMMUNITY

In 2016, Hack the Pentagon was the first ever federal bug bounty program. It was pioneered by the U.S. Department of Defense's Defense Digital Service (DDS) with support from HackerOne. The first iterations were limited to U.S.-based hackers, but as the DDS ran more hacker-powered security programs, they saw the value in inviting hackers from more locations. Subsequent programs were opened up to the so-called "Five Eyes" intelligence alliance countries of Australia, Canada, New Zealand and the U.K. They even allowed a non-NATO country, Sweden, to participate. The results: HackerOne's community of hackers have reported more than 5,000 valid vulnerabilities found in U.S. government systems.

DOWNLOAD NOW

TO LEARN HOW ETHICAL HACKERS HELPED BOLSTER THE SECURITY OF THE U.S. DEPARTMENT OF DEFENSE, DOWNLOAD DEFENDING THE GOVERNMENT FROM CYBER ATTACKS.

Live Hacking Events Bring Hackers and Organizations Together

As organizations look to source more security talent from across the globe, HackerOne makes an effort to get every hacker involved. To meet hackers on their own turf, we organize live hacking events in cities around the world so our customers can interact and engage with the community.

Companies like Uber, Dropbox, Shopify, Oath, and others have all used live hacking events to get face-to-face with security researchers, build relationships, and realize the results of a focused bug-finding effort in just a day or two. Even the U.S. Department of Defense has run a live hacking event, with Hack the Air Force bringing hackers and military security staff together in New York City.

Recent live hacking events have taken place in London, Amsterdam, Singapore, Las Vegas, and other cities around the world. And, more events are planned—maybe even one near you!

Click here to learn how a live hacking event can be the most productive and most exciting one-day penetration test your organization has ever run.

Worldwide HackerOne Events

The Best Talent Probably Isn't Nextdoor

Well over 400,000 hackers make up the HackerOne community. Last year alone they earned nearly US$20 million in bounties, with money flowing from global organizations to reward hackers in Kenya, Algeria, Argentina, Pakistan, Hong Kong, Switzerland, and more than 150 other countries.

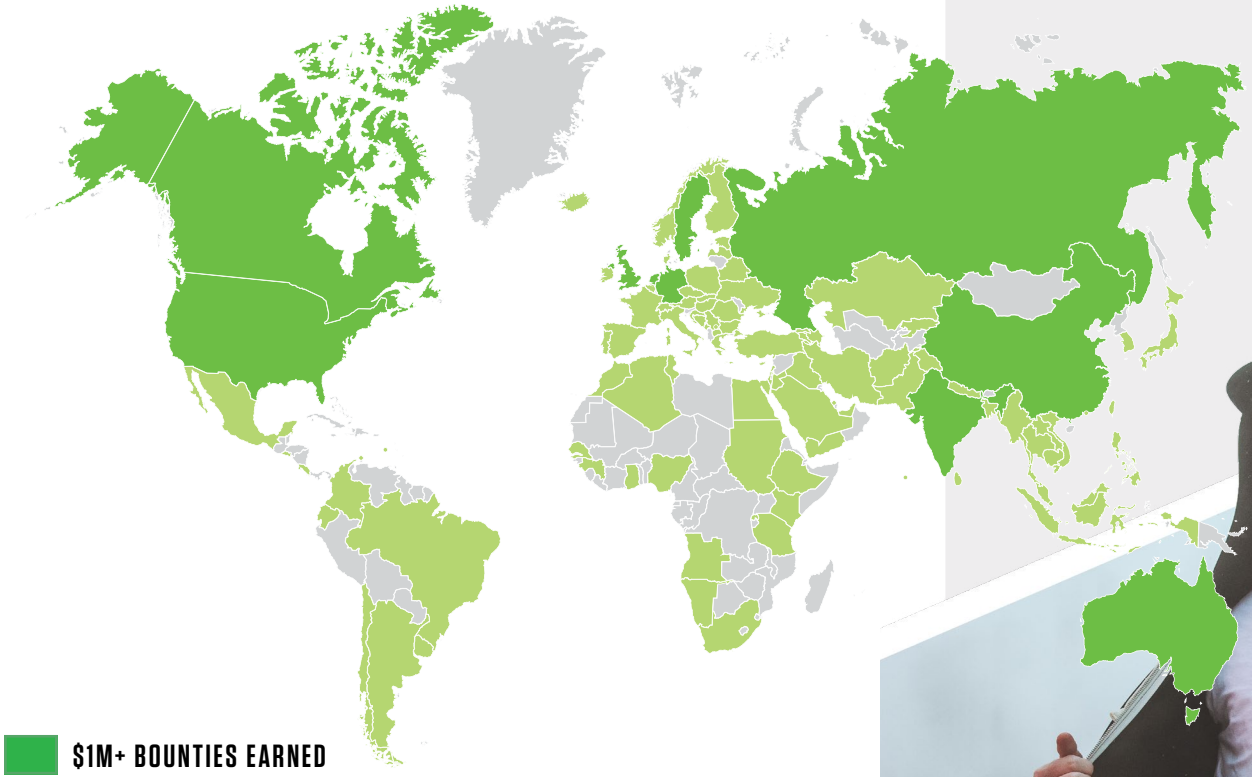
Hacking by the Numbers

400K+
TOTAL REGISTERED USERS

120K+
TOTAL VALID VULNERABILITIES SUBMITTED

$55M+
TOTAL BOUNTIES PAID

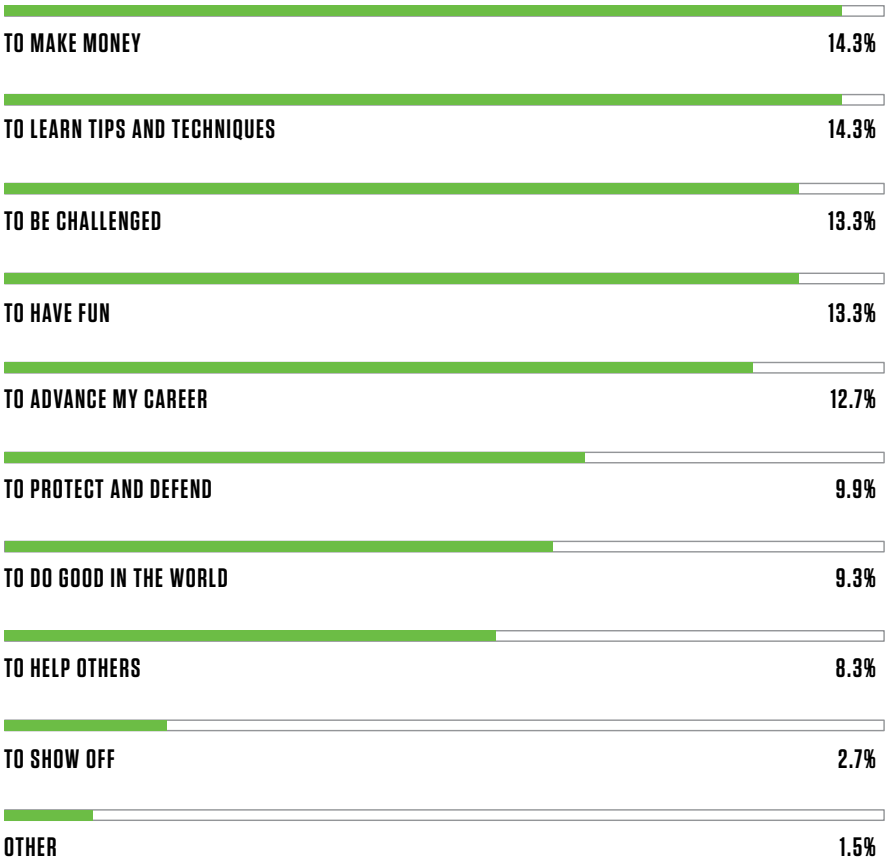
Where HackerOne Hackers Live



$1M+ BOUNTIES EARNED

HACKER PRESENCE

Why Hackers Hack



The hackers helping make the Internet a safer place are educated, professional, curious, and motivated by more than just money. In a recent survey, they noted doing good, helping others, being challenged, and learning new techniques as top reasons for why they hack.

While hackers aren't necessarily in it for the money, it does help. Bounty awards are structured to help attract more of the best hackers and focus their attention where it is needed. Yet rewarding hackers for their effort and validated bug reports makes more economic sense than paying for static test results or having more internal engineers look for bugs.

On the other side of the equation, bounty awards make a huge difference in the lives of hackers across the globe. Top hackers are earning up to 40-times the median annual wage of a local software engineer. That's life-altering money that pulls more of the world's most talented hackers into the HackerOne community, which ultimately benefits the organizations who use hacker-powered security.

Bug Bounties vs. Salary

MULTIPLIER OF MEDIAN ANNUAL WAGE

Median annual wage of a software engineer was derived from PayScale for each region. The multiplier is the top bounty salary divided by the median annual wage of a software engineer.

40.6x ARGENTINA

24.5x THAILAND

24.2x EGYPT

17.6x INDIA

6.7x HONG KONG

6.4x UNITED STATES

3.8x MOROCCO

3.1x BELGIUM

3.0x AUSTRALIA

2.5x ROMANIA

2.2x NETHERLANDS

TO LEARN MORE ABOUT THE 400,000-STRONG HACKER COMMUNITY, DOWNLOAD THE 2019 HACKER REPORT. IT CONTAINS SURVEY RESULTS AND STATISTICS FROM THIS VIBRANT AND GROWING COMMUNITY.

Global Support for Global Security

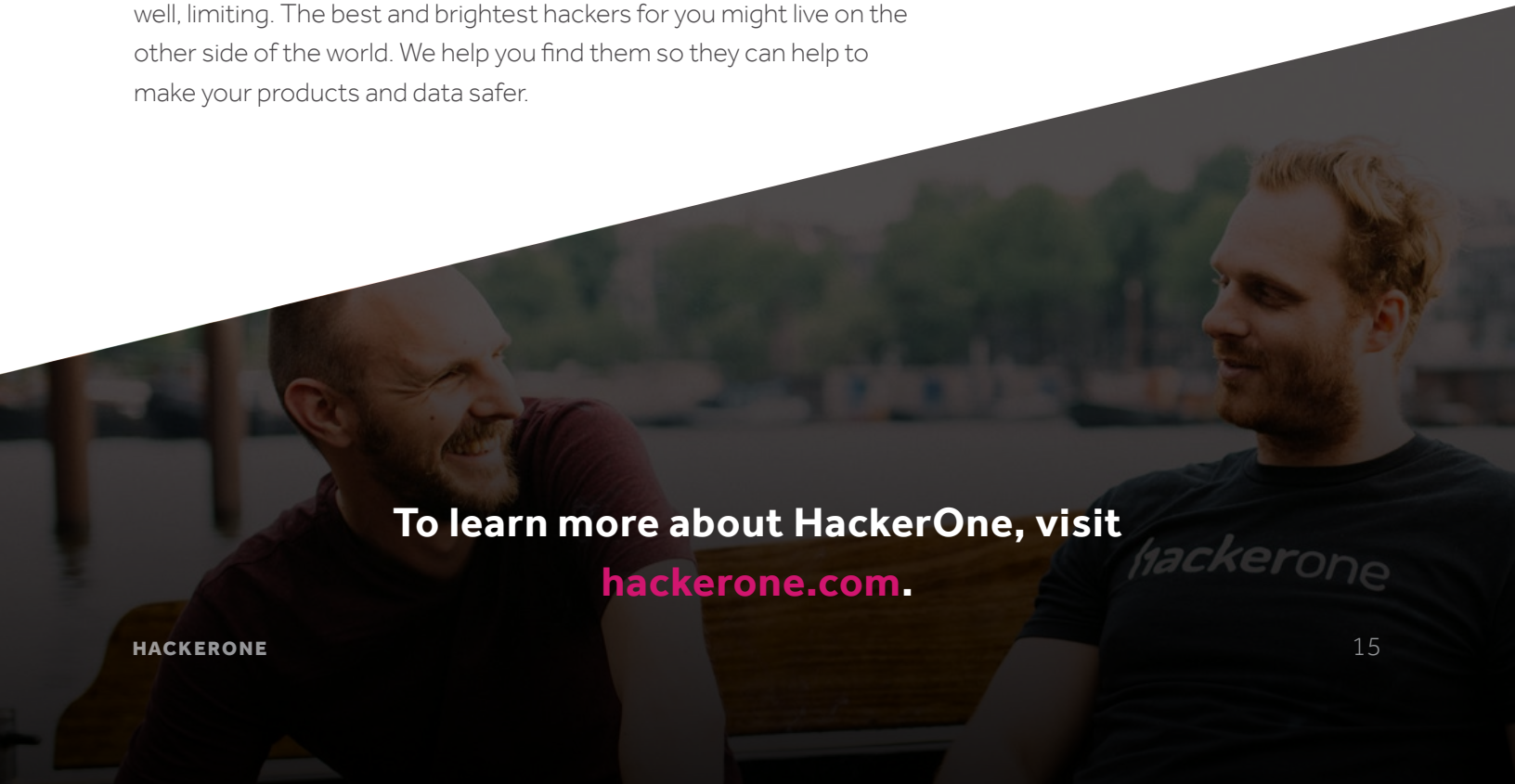
HackerOne was started by hackers and security leaders who are driven by a passion to make the internet safer. We partner with the global hacker community, work with global organizations, and have a global presence. We're headquartered in San Francisco, and have an operational presence in London, New York City, Singapore, and the Netherlands.

We also work with some of the biggest organizations from around the world, many of which we can't mention.

"It's a lot of pride to be a part of a community with such great and smart people."

— MATHIAS
@AVLIDIENBRUNN

Our goal is to surface the most relevant security issues of our customers before they can be exploited by criminals. We know those criminals are relentless, which is why it takes the best hackers to stop them. Limiting your pool of talent to just those in your own region is, well, limiting. The best and brightest hackers for you might live on the other side of the world. We help you find them so they can help to make your products and data safer.



To learn more about HackerOne, visit hackerone.com.