hackerone

The study on the hacker-powered security ecosystem

Executive Summary

According to Gartner, crowdsourced security testing is 'rapidly approaching critical mass'. You will find supporting evidence in this report on the hacker-powered security ecosystem.

A total of 116 bug reports over $10,000 were paid out in the past year with the amount paid for critical issues rising to over $2,000 on average and organizations offering as much as $250,000. Global adoption continues and Latin America is realizing the largest uptake of vulnerability disclosure policies and bug bounty programs, with an increase of 143% year over year. Over $31M has been awarded to hackers as of June 2018 with $11.7M awarded in 2017 alone.

These facts and more are presented in the Hacker-Powered Security Report 2018: the most comprehensive report on hacker-powered security. Data is derived from HackerOne's community of hackers and from platform data for 2017 (defined as May 2017–April 2018) unless otherwise noted. We analyzed 78,275 security vulnerability reports received in the past year from ethical hackers that reported them to over 1,000 organizations through HackerOne.

Organizations remain vastly underprepared for effective discovery, communication, remediation, and disclosure of vulnerabilities as 93% of the Forbes Global 2000 list do not have a policy to receive, respond, and resolve critical bug reports submitted by the outside world. It means we are less safe as a society.

Less than 5% of hackers learn their skills in the classroom—hackers want more education. They want to learn from each other, and explore creative solutions to tough problems. Hackers from over 100 countries have been paid for their research through HackerOne programs, and some are making 16x what they would otherwise be earning as a security engineer in their home country.

Legislators are taking notice and taking action: submitting bills to Hack the DHS, Hack the State Department and inviting expert testimony. 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.

The opportunities and challenges are greater than ever before. As we approach critical mass of hacker-powered security, read on to learn more about best practices of starting and running effective disclosure and bug bounty programs, and get to know some of the stories and stats about the hackers themselves.

> "Crowdsourced security testing is rapidly approaching critical mass, and ongoing adoption and uptake by buyers is expected to be rapid..."

GARTNER EMERGING TECHNOLOGY ANALYSIS:
Bug Bounties and Crowdsourced Security Testing, June 2018

Introduction

Hackers are in high demand for their ability to forewarn and safeguard against criminal attacks. We've learned from years of breaches and lost trust that we need to get smarter to protect our digitally connected society. Security teams need the tools and resources to keep up with the speed of software development and evolving threats.

Today we see that relying on compliance, checking boxes and purchasing the latest security products only gets you so far. A scanner can't find a vulnerability it doesn't know exists. Creative intellectual humans do that. Hackers do that.

We're honored to tell some of their stories, showcase how they think, what they hunt, and what motivates them. We have the most compelling hacker stories to tell, because we have the largest and most active hacker community in the world. They act as a valued extension of our customers security teams—on a mission to find what others may have missed or could not see.

Our customers are encouraged to build relationships with and hire hackers. The Security@ industry conference and our live hacking events are the most poignant examples of this, bringing security teams and hackers together in the same venue. We're building bridges not erecting walls and forcing conversations to go through an intermediary. The results demonstrate the power of the collective community that together, we can solve problems better, faster, and cheaper.

We have a saying, "Together We Hit Harder," that you'll see in our materials, embraced by our hackers, and championed by our staff. It is our mission to empower the world to make the internet safer. This report is a glimpse into how we go about doing just that.


hackerone
hackerone
hackerone

Contents

Important Terms

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

Hacker-Powered Security: Any 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 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.

Hacktivity: Hacker activity published on the HackerOne platform.

Public Bug Bounty Program: An open program any hackers 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 program with a pre-determined limited time frame. In most cases hackers will register or be invited.

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. 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

- **Critical vulnerabilities are earning higher bounties.** The average award for a critical vulnerability increased 33% to $20,000 for the top awarding programs. A total of 116 unique critical vulnerabilities earned over $10,000 each in the past year.

- **Bug bounty earning potential is changing lives.** Hackers in over 100 countries have taken home $31M to date. The top earning hackers made 2.7x the median salary of a software engineer in their home country, some make up to 16x.

- **Governments are leading the way with adoption globally.** The U.S. Department of Defense has received over 5,000 reports since the launch of their vulnerability disclosure policy and conducted another three time-bound bug bounty challenges in the same model as 'Hack The Pentagon". The Singapore Ministry of Defense and the EU Commission also launched public programs.

- **Valid reports hit an all-time high as program signal becomes a primary program performance metric.** The fear of program noise (ie, informative or duplicate submissions) is a relic of the past across hacker-powered programs. With a platform-wide signal of 80%, the human resources required to run a hacker-powered program were greatly reduced in 2018.

- **Adoption of of vulnerability disclosure policies (VDP) are on the rise across Enterprise organizations.** Goldman Sachs, Toyota, and American Express were a few of the enterprises to launch a VDP in 2018. Overall, HackerOne saw a 54% year-over-year increase in new Enterprise VDP program launches, however, the adoption of the Forbes 2000 only marginally improved. Today, 93% of the Forbes 2000 still do NOT have a public-facing VDP.

- **Less than 5% of hackers learn to hack in the classroom.** Hacker education has improved greatly in the past year with online resources such as Hacker101.com and HackEDU.io being a couple excellent examples. But the need for structured curriculum in high schools and colleges nationwide remains evident with 25% of the hacker community currently enrolled as a full-time student.

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

2013

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

2016

April: Hack the Pentagon pilot bug bounty program launches

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.

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: 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

2017

May : Hack the DHS bill passed Senate

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 | **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:** US Department of Justice publishes A Framework for a Vulnerability Disclosure Program for Online Systems.

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 | **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 proposed 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) introduced "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 | **June:** HackerOne exceeds $30,000,000 in bounties paid out to hackers.

Hacker-Powered Program Adoption and Bounties by Geography

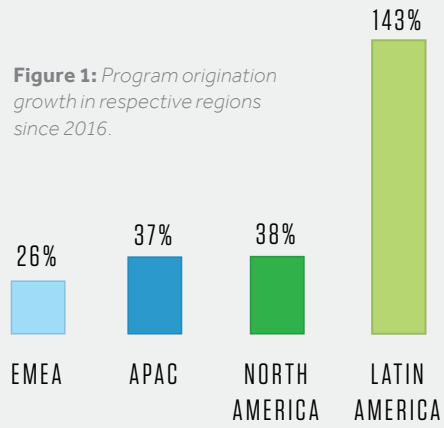
The number of hacker-powered security programs continues to be a global phenomenon, with double or triple-digit growth on every populated continent. Of all the regions, **Latin America had the largest uptake of VDPs and bug bounty programs, with an increase of 143% year over year**. North America and the Asia Pacific region each increased 37%, and Europe, the Middle East, and Africa saw a combined 26% increase in the past year.

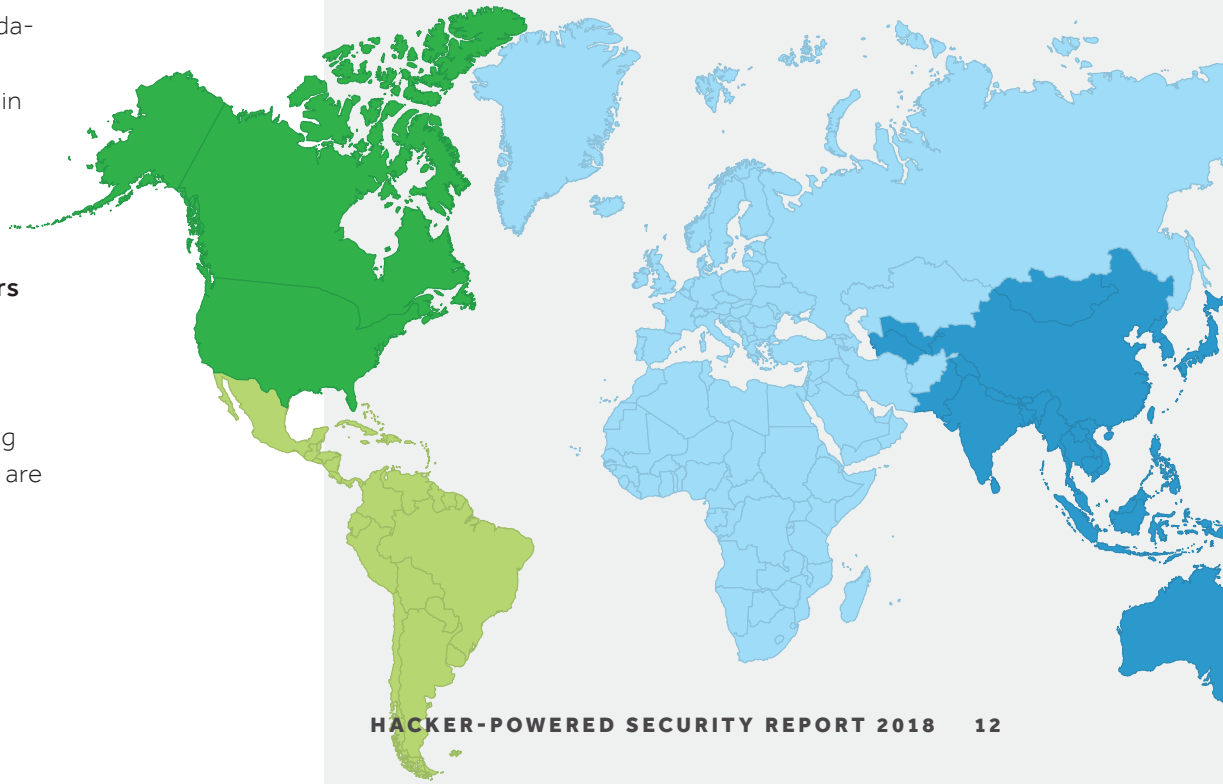
Organizations located in the U.S. continue to pay the highest volume of bounties to hackers around the globe (83%). Canada-based organizations remain in the second spot for 2017, with $1.5 million paid, while those in the U.K. rose from sixth place in 2016 to third place this year.

Talented hackers earning bounties are from all over the world. Eighteen unique countries have hackers earning a combined $500,000 or more, and 44 countries have hackers earning a combined $100,000 or more as of April 2018.

Hackers in the U.S. earned 17% of all bounties awarded, with India (13%), Russia (6%), U.K. (4%), and Germany (3%) rounding out the top 5 highest-earning countries. Hackers in Germany are on a roll, earning 157% more in 2017 versus 2016.

Figure 1: *Program origination growth in respective regions since 2016.*





Bounties by Geography

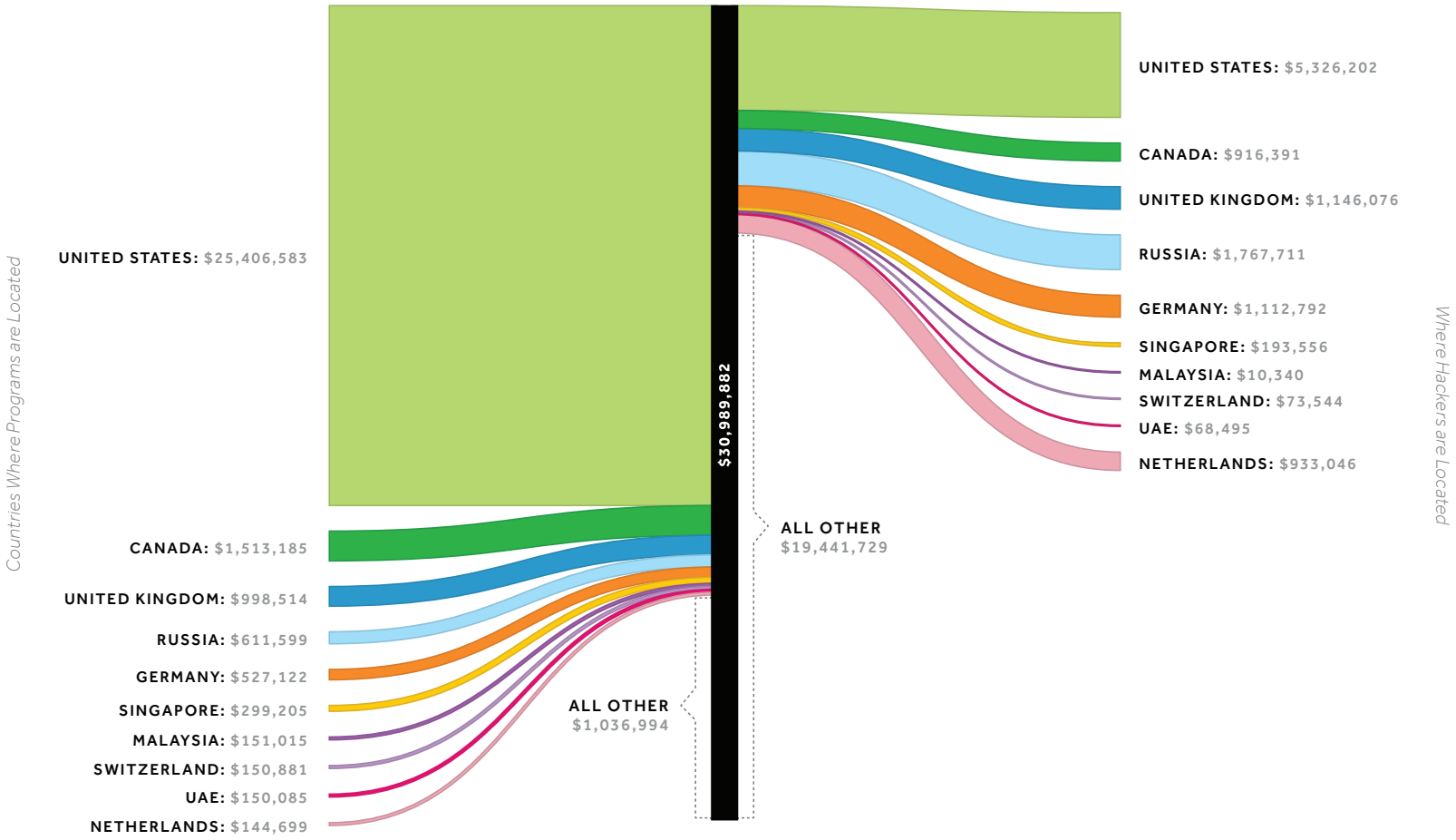


Figure 2: *Visualization of the Bounties by Geography showing on the left where the companies paying bounties are located and on the right where hackers receiving bounties are located.*

Public vs. Private Bug Bounty Programs

The bug bounty program is the most advanced form of hacker-powered security. It is for those with mature security postures, ready to adopt continuous security testing from the most scrutinizing of hackers. Bug bounty programs can be either public or private. Public programs (examples include Starbucks, GitHub, and Airbnb) are open to everyone, and private programs require individual hackers to be invited or accepted through an application process in order to participate. Public bug bounty programs represent the highest hacker diversity and therefore produce superior results. On average, **public programs engage 3.5 times the number of hackers reporting valid vulnerabilities.**

Private bug bounty programs currently make up 79% of all bug bounty programs on HackerOne, down from 88% in 2017 and 92% in 2016 calendar years, meaning more programs are going public on HackerOne. The majority of public bug bounty programs are from Technology (63%) followed by Financial Services and Banking (9%) and Media and Entertainment (9%) industries. In contrast, nearly 100% of programs are private in the Consumer Goods, Healthcare and Telecommunications industries.

Public programs made up about 19% of HackerOne bug bounty launches in the past 12 months, about double compared to the year before.

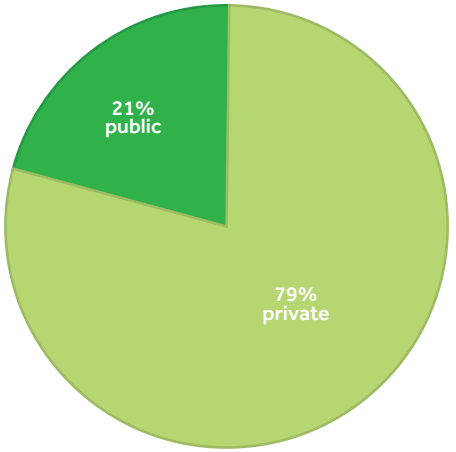


Figure 3: *Percentage of bug bounty programs that are public and private as of 2017*

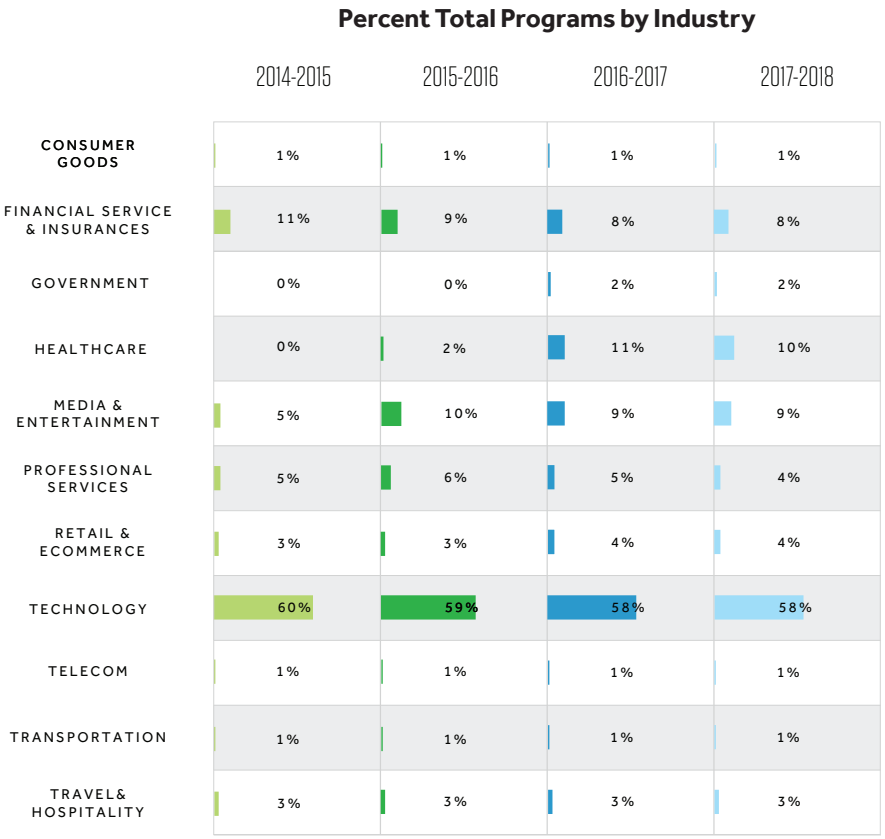


Figure 4: *Industries that launched programs from the overall share of programs for that time period.*

Bug Bounty Program Adoption by Industry

For the fourth year in a row, industries beyond Technology increased their share of the overall bug bounty market. While Technology companies still lead the pack, non-technology industries like Consumer Goods, Financial Services & Insurance, Government, and Telecommunications account for 43% of today's bug bounty programs. Notably, **Automotive programs increased 50% in the past year and Telecommunications programs increased 71%.**

In the government sector there was 125% increase year over year globally with new program launches including the European Commission and the Ministry of Defense Singapore, and others. The U.S. Department of Defense completed new time-bound bug bounty challenges for the U.S. Army, U.S. Air Force and Defense Travel System over the past year paving the way for hacker-powered security legislation like Hack DHS and Hack the Election. The results from these programs and recommendations from regulators demonstrate that **hacker-powered security programs are a fast and reliable way to secure digital assets for the public sector.**

Vulnerabilities by Industry

More than 72,000 vulnerabilities have been resolved on HackerOne as of May 2018, with more than one-third of those—27,000—resolved in the past year alone.

Taking a close look at the top 15 vulnerability types reported on HackerOne, cross-site scripting (XSS, CWE-79) continued to be the most common vulnerability across all industries, with the exception of Healthcare and Technology.

For Healthcare and Technology industries, of the top 15 vulnerability types reported, nearly 8,000 were related to Information Disclosure (CWE-200). These are instances when information is disclosed to an actor that is not explicitly authorized to have access to that information. This ranges from sensitive information within the product's own functionality—a private message, for example—to information about the product or its environment that is not normally available to an attacker, such as the installation path of a product that is remotely accessible. Severity of Information Disclosure bugs ranges from low severity to critical.

Vulnerabilities submitted by hackers are ranked in severity as either low, medium, high, or critical as part of the scoring process. At HackerOne, the severity of every security vulnerability is measured with Common Vulnerability Scoring System framework (CVSS) v3.0. For 2017 the total number of critical vulnerabilities reported increased by 26%. The share of the most impactful bugs—critical and high combined—increased from 22% in 2016 to 24% in 2017.

XSS vulnerabilities represented 59% of the top 15 vulnerabilities reported to Transportation organizations and 37% of the top 15 vulnerabilities reported to Travel & Hospitality organizations.

SPOTLIGHT

Trending Vulnerability Spotlight: S3 Buckets and Security in the Cloud

There has been a significant rise in security incidents as a result of insecure storage vulnerabilities. The most popular of which is Amazon Simple Storage Service (often referred to as S3 Buckets). S3 Buckets are typically used by IT departments to store source code, certificates, passwords, and other data. Misconfigurations have exposed names, addresses, credit scores, partial Social Security numbers, and allowed for man-in-the-middle attacks. Recent incidents with auto loan, telecommunications, and entertainment organizations have affected as many as 17 million consumers. Over the past year, there has been a stark increase in vulnerabilities related to Insecure Storage of sensitive information. In fact, **there were 38 times more insecure storage vulnerabilities reported in 2017 compared to 2016** on HackerOne.

Vulnerabilities by Industry

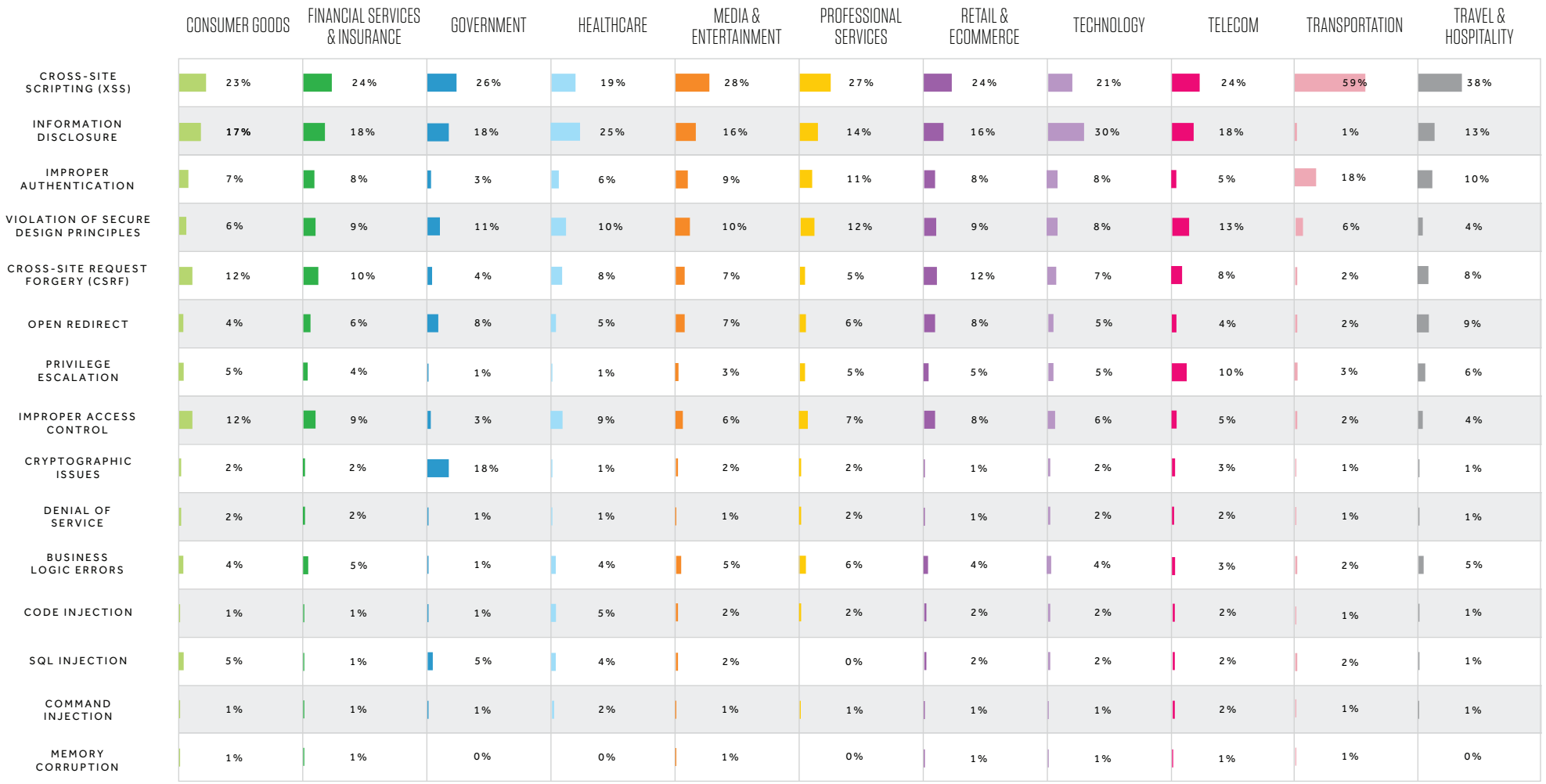


Figure 5: *Listed are the top 15 vulnerability types platform wide, and the percentage of vulnerabilities received per industry.*

CUSTOMER SPOTLIGHT

General Motors

Global automotive company General Motors, known for iconic brands like Chevrolet, Cadillac, and Buick became the first major automaker to launch a public vulnerability disclosure program (VDP) in 2016. Its purpose? To protect its customers by working with hackers to safely identify and resolve security vulnerabilities. In just two years, GM has resolved more than 700 vulnerabilities across the entire supply chain, with help from over 500 hackers.

"We're taking cybersecurity very seriously at General Motors. It's a top priority for our company, and our most senior executives, including the CEO, fully support our organization," said Jeff Massimilla, Vice President Global Cybersecurity at GM. "We are employing strategies and programs, like our VDP with HackerOne, with the sole purpose of protecting our customers, their vehicles and their data."

Seven of the top 50 automotive vehicle manufacturers globally have a way for external researchers to report vulnerabilities. Four of these seven fall under the GM brand: Buick, Cadillac, Chevrolet and GMC. Furthermore, only two of the top 50 suppliers of the automotive industry (Johnson Controls Inc. and BASF SE) have a channel for disclosure.

"We've always approached security with a diverse set of tools in our toolbox," said Massimilla. "Leveraging HackerOne's relationship with the research community, and seeing firsthand the results they provide, has been extremely encouraging. Hackers have become an essential part of our security ecosystem."

> "Hackers have become an essential part of our security ecosystem.

JEFF MASSIMILLA

Vice President Global Cybersecurity, GM

VULNERABILITIES RESOLVED
700+

COMPANY HEADCOUNT
180,000+

PARTICIPATING HACKERS
500+

PRODUCT
HackerOne Response

As of March 2018

Time to Resolution by Industry

Time to resolution is the number of business days it takes for a security team to resolve a reported bug and a key indicator of program health. It is the primary metric that shows hackers what they can expect from the program. Security teams can also measure their own success by setting goals around average time to resolution for their program. With 27,000 valid reports resolved in 2017 on HackerOne alone, and 78,275 total reports submitted, facilitating this process from report to resolution is the primary role of HackerOne Services, which is used by many HackerOne customers.

The best—in other words, the fastest—industry with respect to average resolution times are Consumer Goods (14 days), Financial Services & Insurance (19 days), and Healthcare (20 days). Resolution times by industry then jump to Technology (64 days), Transportation (65 days), and Government (68 days) organizations. There are a variety of reasons why resolution times vary from industry to industry, organization to organization. This can include complex technology stacks or supply chains that require coordination with partners and other vendors, as is typically the case for Telecommunications and Transportation organizations.

Once an issue is resolved, a bounty should be paid shortly thereafter—if not at the time of validation. This ensures not only hacker satisfaction, but that the organizational mechanisms for facilitating payment are aligned with the value provided by the hackers who identify the vulnerabilities.

The industries with the fastest average days to bounty payment are Healthcare (15 days), Government (18 days), and Financial Services & Insurance (19 days). On the other end of the spectrum, the industries with the slowest days to bounty payment are Professional Services (47 days), Telecommunications (51 days), and Travel & Hospitality (61 days).

Notice that the Healthcare industry tends to pay hackers before issues are resolved (but after they are validated), and Government organizations tend to pay well before issues are resolved. Other industries can take up to 31 days (Travel & Hospitality), on average, to pay bounties after an issue is resolved.

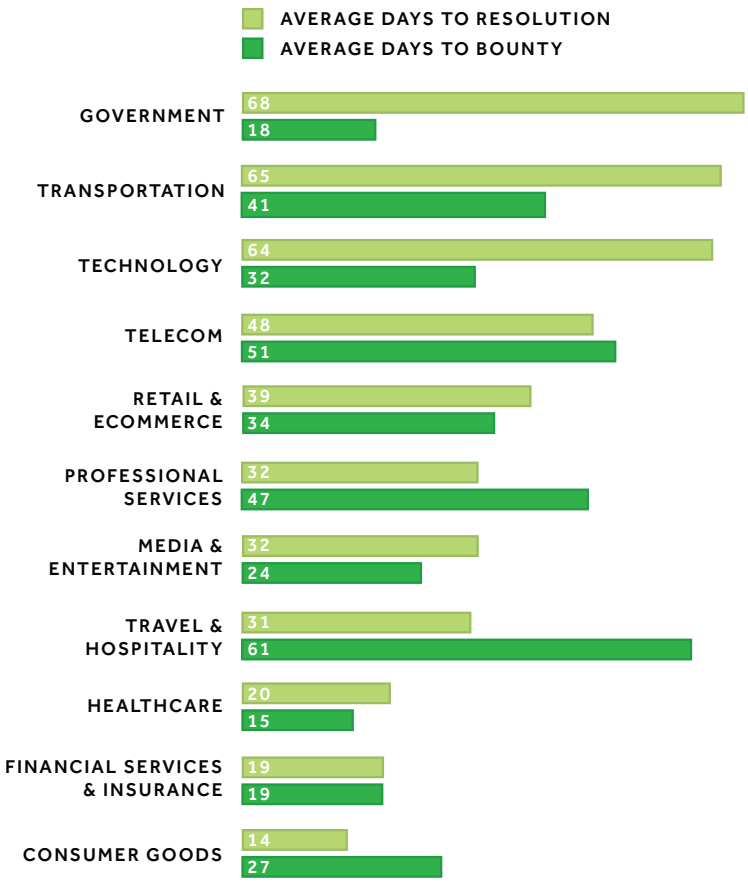


Figure 6: *Average number of days to resolution and to reward, measured from May, 2017 to April, 2018.*

Cybersecurity Statistics

7,000

Each year 5,000 to 7,000 different new exploits appear.
CSO

3.5 million

The number of unfilled cybersecurity jobs will triple to 3.5 million by 2021.
CSO

350%

Ransomware is growing at a yearly rate of 350%, according to the Cisco 2017 Annual Cybersecurity Report.
Cisco

301,000

U.S. National Institute of Standards and Technology reports that there are currently "over 301,000 open jobs in cybersecurity across the nation, including over 13,000 openings in the public sector."
NIST

$6 trillion

Cyber crime will cost organizations worldwide $6 trillion annually by 2021, up from $3 trillion in 2015.
CSO

50%

By 2022, (hacker-powered security) will be employed by more than 50% of enterprises
Gartner

Bounty Trends: Severity

About 60% of organizations on the platform pay an average of $1,500 for critical vulnerabilities, which is a 50% ($500) increase from 2016 for average bounties paid for critical vulnerabilities. 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 the HackerOne platform rose to $2,041 in 2017. That's a 6% YoY increase over the 2016 average of $1,923.

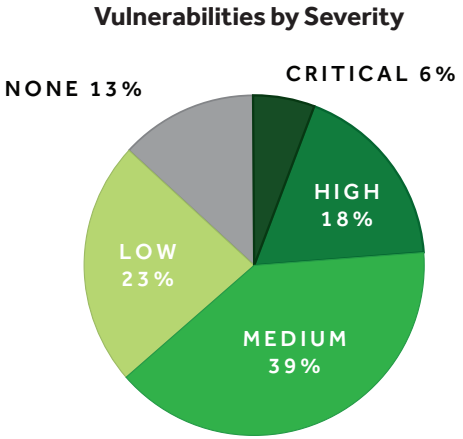


Figure 7: *The percentage of all vulnerabilities that are categorized as critical, high, medium or low severity. The "none" category represents vulnerabilities that did not register on the severity scale.*

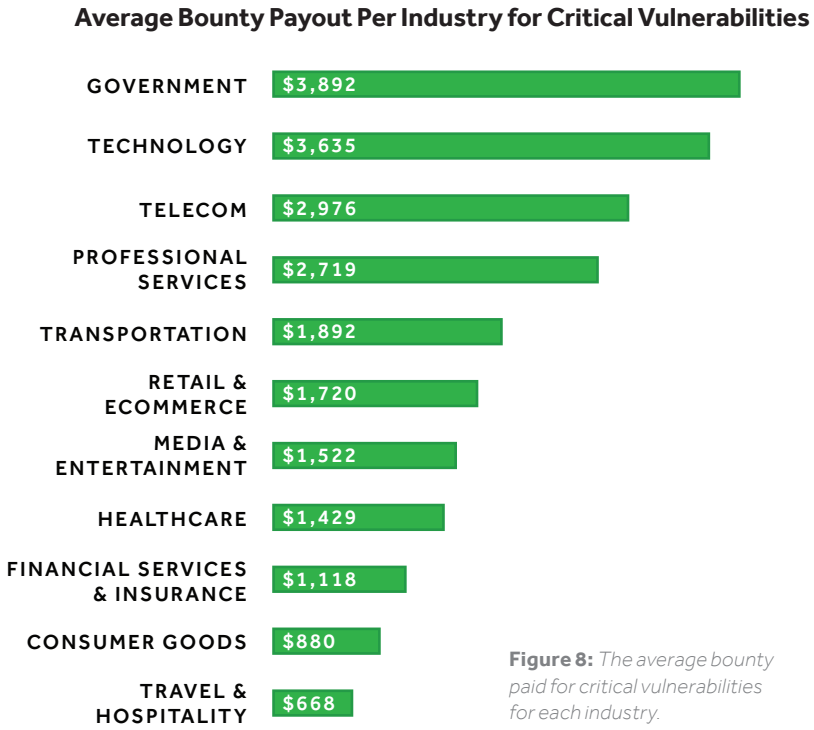
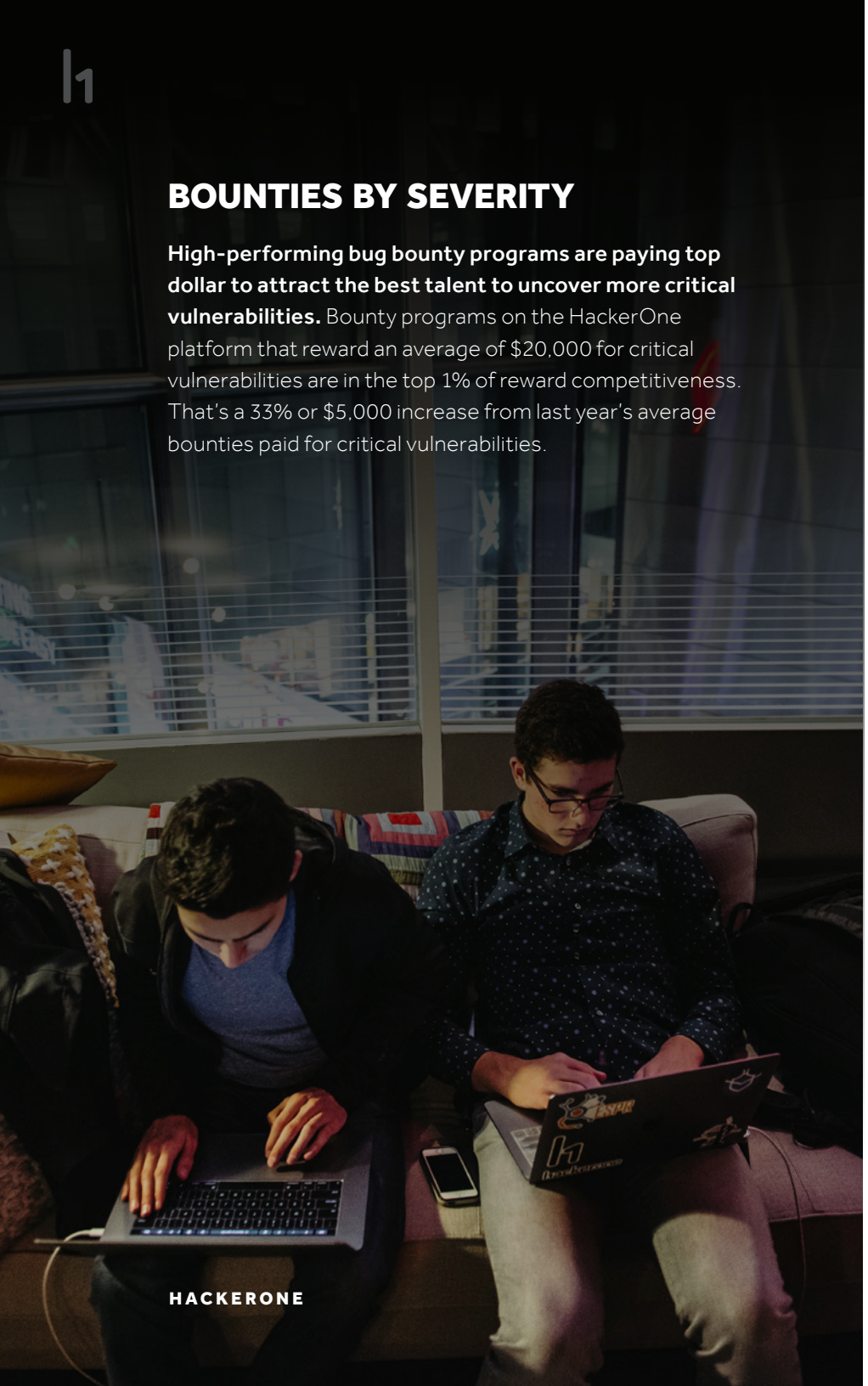


Figure 8: *The average bounty paid for critical vulnerabilities for each industry.*



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 the HackerOne platform that reward an average of $20,000 for critical vulnerabilities are in the top 1% of reward competitiveness. That's a 33% or $5,000 increase from last year's average bounties paid for critical vulnerabilities.

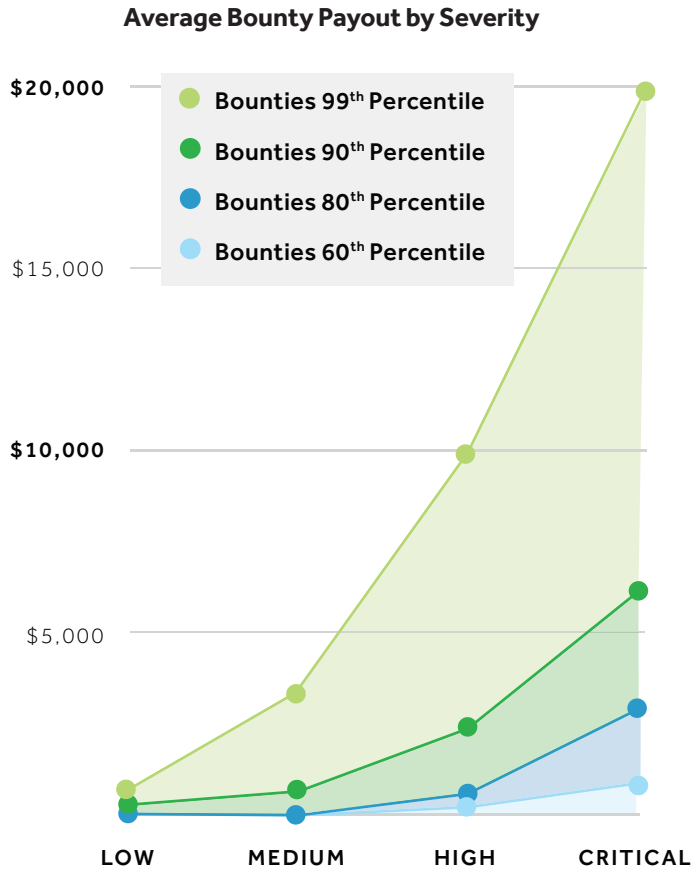


Figure 9: *Bug bounty reward competitiveness for critical vulnerabilities from May 2017 to April 2018. Organizations in the 99th percentile, rewarding $20,000 on average, are rewarding bounties higher on average than 99% of the programs on HackerOne.*

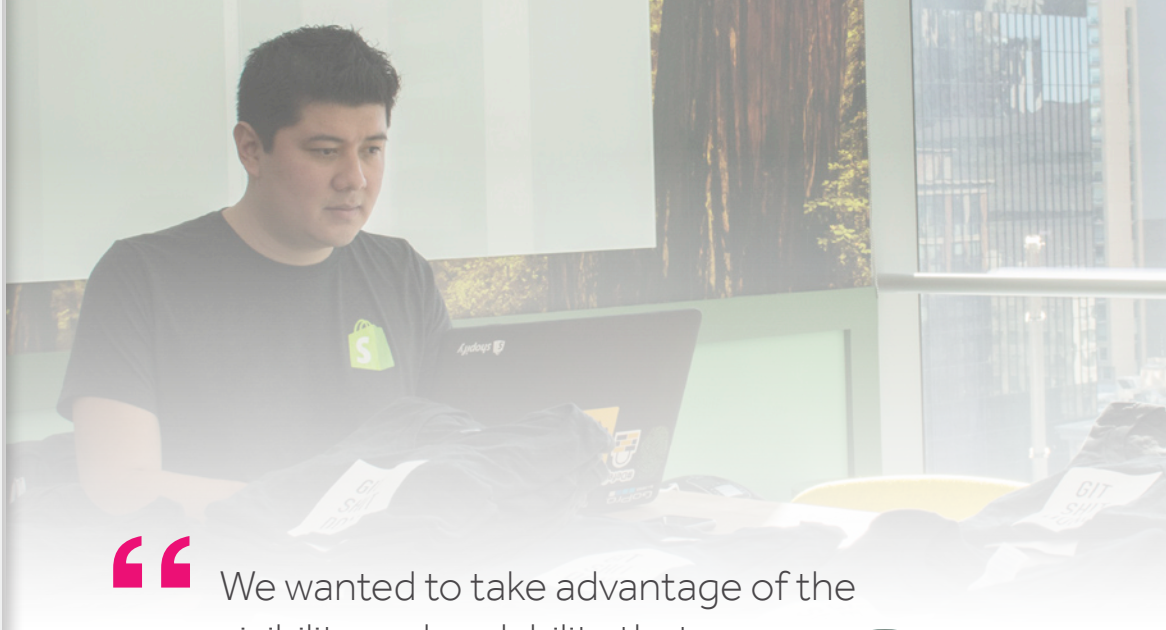
CUSTOMER SPOTLIGHT

Shopify

E-Commerce leader Shopify currently powers over 600,000 businesses in approximately 175 countries and is trusted by brands such as Red Bull and Nestle. Shopify has resolved 759 vulnerabilities and awarded more than 300 hackers over $850,000 in just over three years. To date Shopify has an all-time average first response time of just 3 hours and an average resolution time of just 25 days. This places Shopify among the most responsive and highest paying programs on HackerOne.

"We want to be known for being one of the most responsive companies and also pay top dollars for top findings," said Tobi Lutke, CEO of Shopify. "It should be more fun and more lucrative to make Shopify-related discoveries than (for) other companies."

In 2017, Shopify hired one of HackerOne's top 100 hackers, Pete Yaworski, for a full time role on their security team, a relationship that was established at the H1-415 2017 live-hacking event in SF.



"We wanted to take advantage of the visibility and scalability that came with HackerOne.

ANDREW DUNBAR

Director, Risk & Compliance, Shopify

VULNERABILITIES RESOLVED

759+

COMPANY HEADCOUNT

3,000+

PARTICIPATING HACKERS

300+

PRODUCT

HackerOne Bounty

As of April 2018

Bounty Trends: Top Awards

From HackerOne's inception in 2012 through June 2018, organizations have awarded hackers over $31 million. More than one-third of that, **$11.7 million, was awarded in the past year alone**, reflecting the striking growth trajectory of hacker-powered security.

Some of the most advanced organizations offer bounty awards in the six-figure range, with Intel and Microsoft offering up to $250,000, and Google and Apple offering up to $200,000, to name just a few. Bounties for critical severity vulnerabilities in the tens of thousands of dollars is not only common, it's expected for more mature bug bounty programs.

The highest bounty paid in 2017 was $75,000, paid by a Technology company for three unique vulnerabilities that when chained together produced a remote code execution (RCE) that required no user interaction to exploit. The exploit chain could have allowed an attacker to steal credit card information, deploy mass ransomware campaigns, take over user accounts, attack employee accounts and access infrastructure code. These are the types of critical issues that are found exclusively with hacker ingenuity.

In just the past year, organizations in the Transportation, Telecommunications, Professional Services, and Technology industries all awarded top bounty awards of $20,000 or more. **Across all industries, 116 individual bounties over $10,000 were awarded. That's up more than 30% from 2016.**

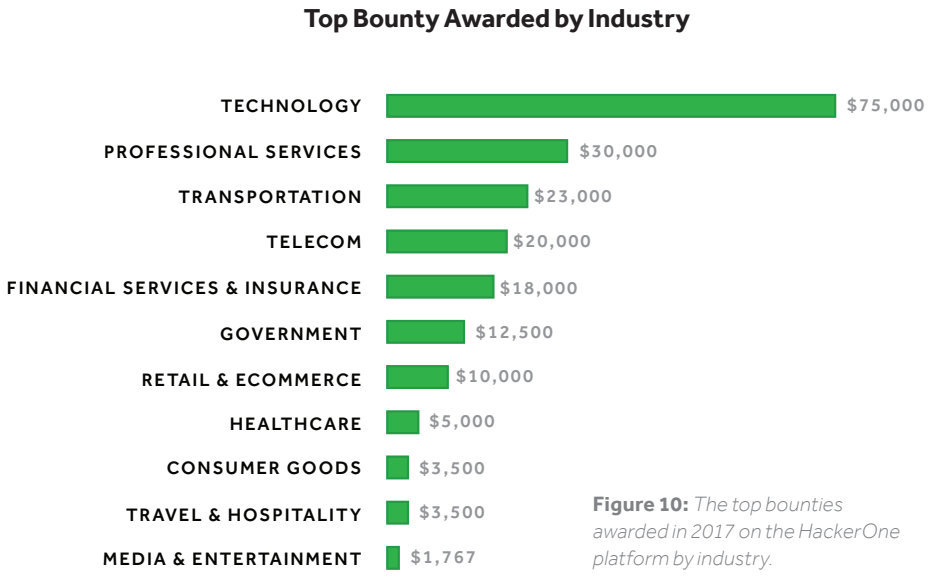


Figure 10: *The top bounties awarded in 2017 on the HackerOne platform by industry.*

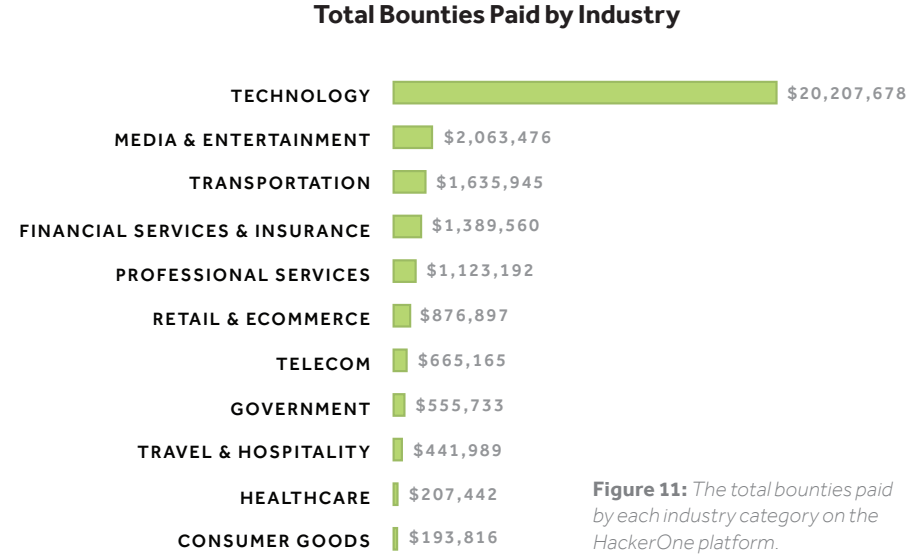


Figure 11: *The total bounties paid by each industry category on the HackerOne platform.*

Oath

In April 2018, 41 hackers representing 11 countries were in San Francisco hacking Oath, a media and tech company that includes: Yahoo, AOL, Verizon Digital Media Services, TechCrunch, and many more dynamic brands. In just nine hours of hacking, Oath awarded hackers over $400,000 in bounties. This live hacking event was dubbed H1-415, with 415 representing the San Francisco area code.

"Surfacing vulnerabilities and resolving them before our adversaries can exploit them is essential in helping us build brands people love and trust," said Chris Nims, CISO at Oath. "Whether they had been participating in our programs for years or were looking at Oath assets for the first time, it was empowering to witness the dedication, persistence and creativity of the hacker community live and in person. We really felt the excitement and enthusiasm throughout H1-415."

The Oath security team huddled shoulder to shoulder with hackers to work together, assess impact, payout rewards, and resolve vulnerabilities in record time. This was the first time Oath introduced its consolidated private bug bounty program, following its acquisition of Yahoo in 2017. The speed and agility of the security team demonstrated next level security maturity and readiness to efficiently handle security vulnerabilities.

> It was empowering to witness the dedication, persistence and creativity of the hacker community live and in person.

CHRIS NIMS
CISO, Oath

VULNERABILITIES RESOLVED
700+

COMPANY HEADCOUNT
180,000+

PARTICIPATING HACKERS
950+

PRODUCT
HackerOne Bounty

As of October 2017

Signal-to-Noise Ratio

Signal-to-noise is a quantitative measure of a program's submission quality based on the validity of incoming reports. Signal indicates the number of valid reports received, while noise is the share of non-valid reports received. 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, signal-to-noise was often an obstacle to overcome in order for organizations to be successful. 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 number is brought closer to 100% signal. That means the total cost of ownership is dropping fast and hacker-powered security is within everyone's reach.

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.

80% PLATFORM-WIDE SIGNAL

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 marked "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

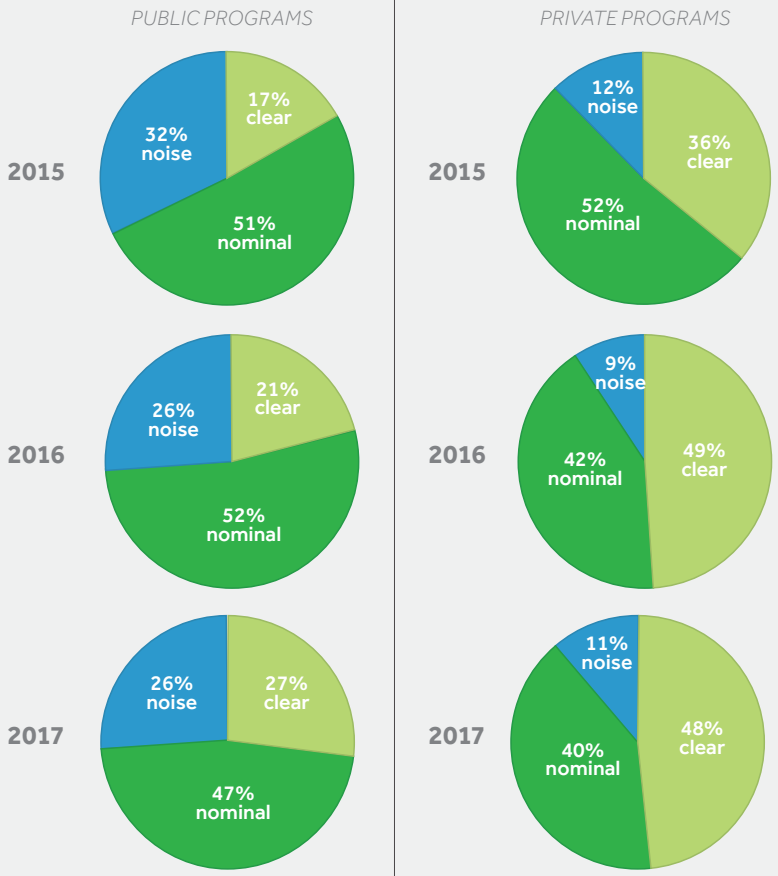


Figure 12: *Historical signal-to-noise ratios on the HackerOne platform*

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 over time.

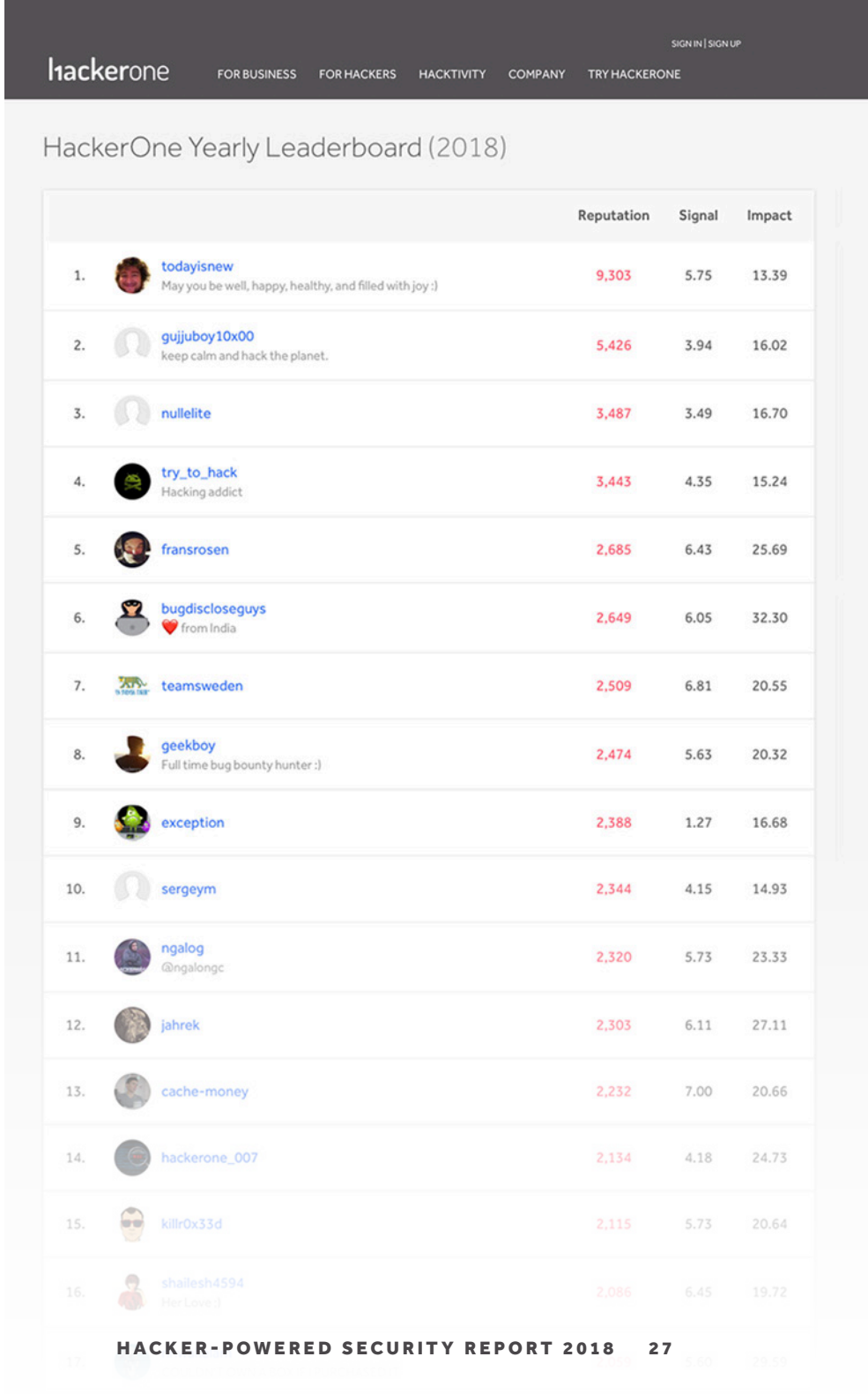
Tracking Hacker Signal

The HackerOne Platform allows you to privately invite a select group of hackers in a safe and controlled manner. Hacker activity and productivity is tracked in 3 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%.

While eliminating all noise is improbable we've set ourselves a target to reach 90% signal—a standard that hasn't been seen on any other platform in our industry. Currently HackerOne consistently maintains 80% Signal platform wide.



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 Reputation metrics, past program participation, specific skills, and more. How does it work?

Step 1. Identify and select hackers based on their activity on other bounty programs, as well as their Signal, Impact, and Reputation scores. Hacker activity and submission quality is tracked and incorporated into their Reputation.

Step 2. Work with HackerOne to find the right hackers with the skills you need. Each hacker's profile page contains not only their Reputation metrics, but also their "hacktivity", number of bugs found and thanks received, and badges earned. This offers a unique view into the skills and experience of each hacker, since hacktivity shows all previously resolved reports and, if public, the details of the actual report. Hackers can also add skills to their profile by submitting relevant reports.

Step 3. Partner with your HackerOne Program Manager to determine if there are custom requirements you'd prefer to explore including: NDAs, a robust application process, and even background checks.

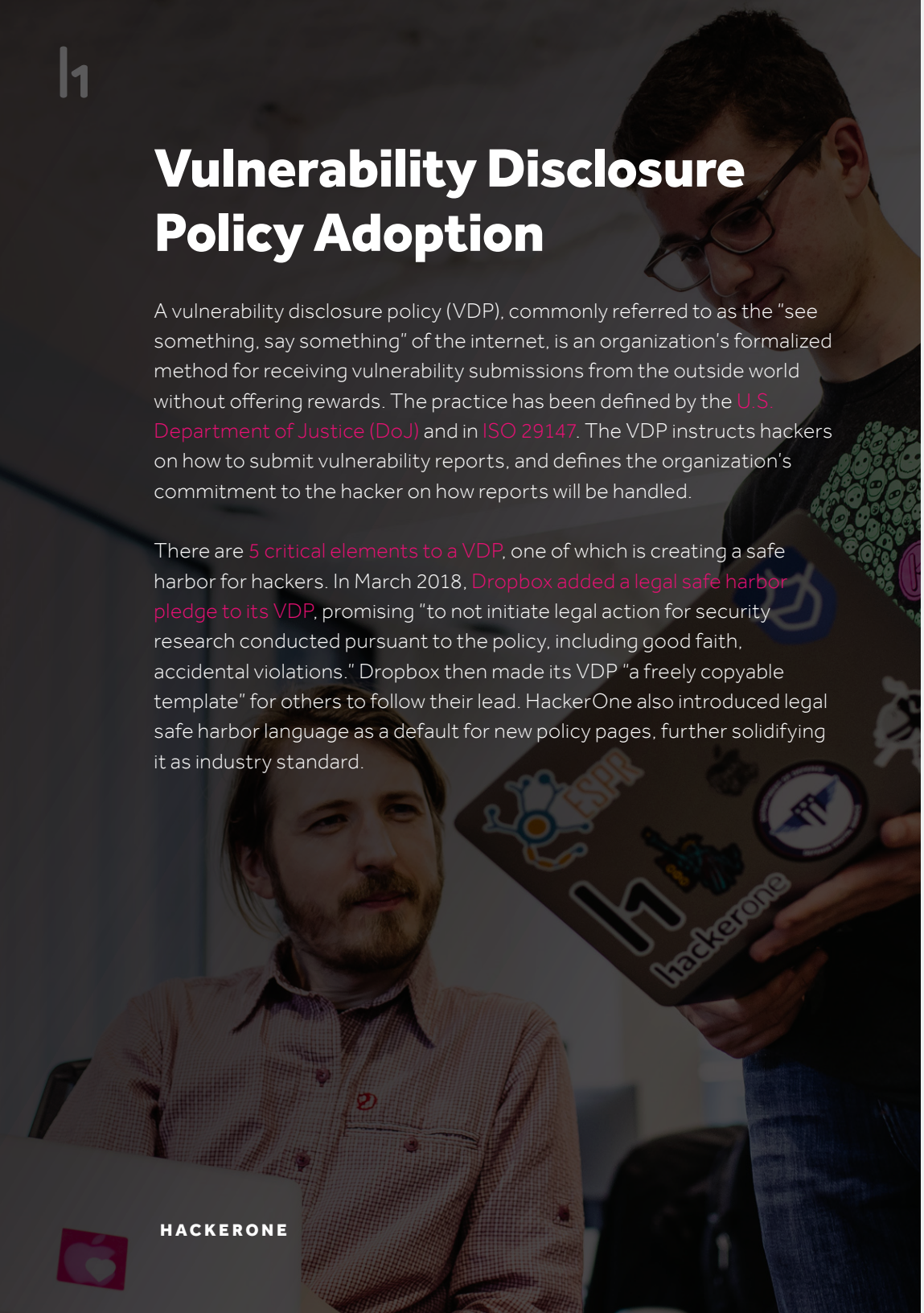
Want the most scrutinizing of programs? Then you need HackerOne Clear. HackerOne Clear hackers meet the strictest background and identity standards of the most demanding global organizations, such as the U.S. Department of Defense. Contact us to learn more.

SAMPLE HACKER PROFILE

Sean Melia (meals)

SENIOR SECURITY ENGINEER, GOTHAM DIGITAL SCIENCE
@seanmeals | Member since September 24th, 2014

REPUTATION		CREDIT
5.48 Signal	93RD Percentile	876 Bugs Found
17.36 Impact	88TH Percentile	80 Thanks Received
20033 Reputation	5TH Rank	



Vulnerability Disclosure Policy Adoption

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 vulnerability submissions from the outside world without offering rewards. The practice has been defined by the U.S. Department of Justice (DoJ) and in ISO 29147. 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.

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.

Legal Experts and Market Leaders Embrace VDPs

"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, Vice President Global Cybersecurity at GM.

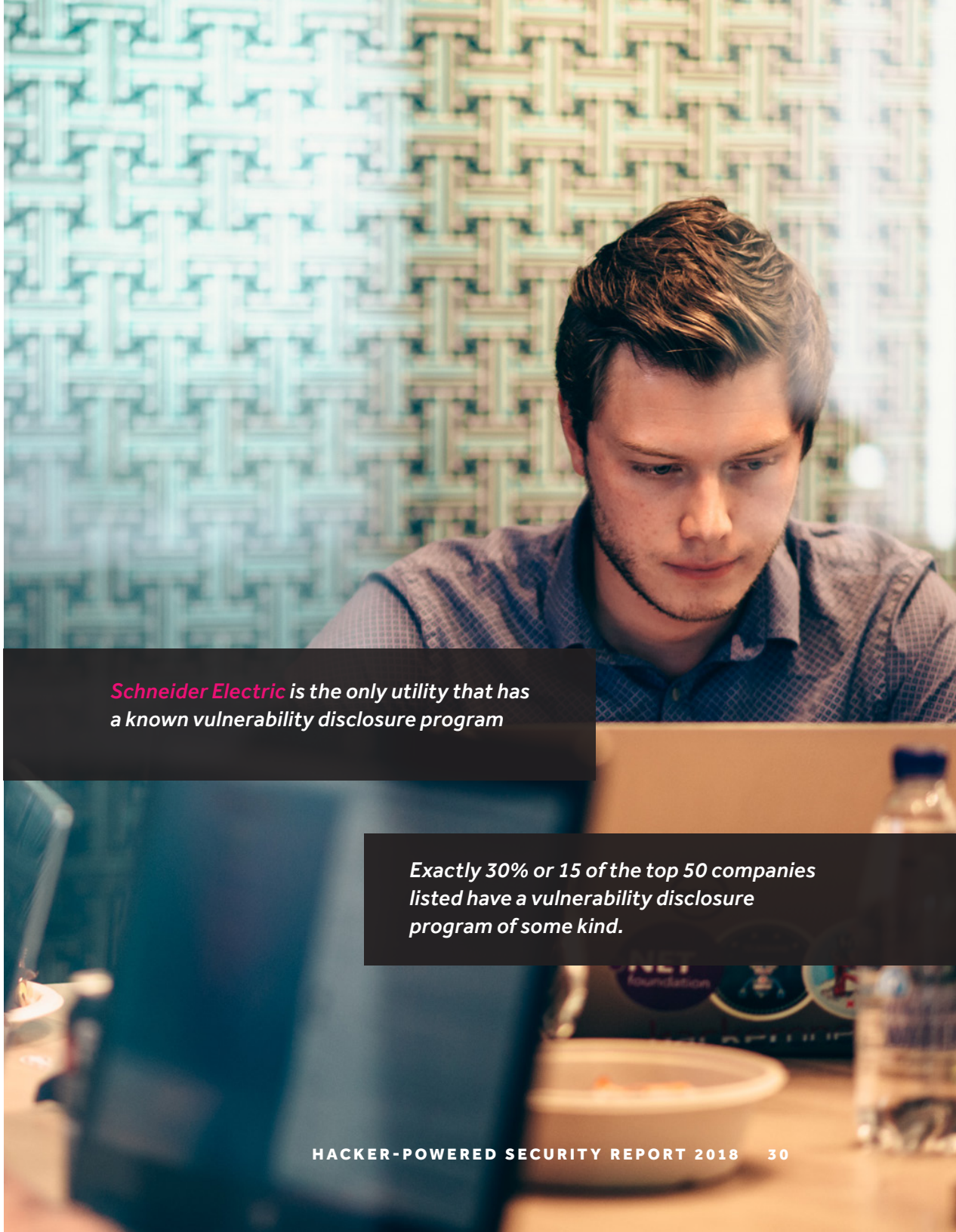
"All companies should consider promulgating a vulnerability disclosure policy, that is, a public invitation for white hat security researchers to report vulnerabilities found on your system," said Rod Rosenstein, Deputy Attorney General. "The Department of Defense runs such a program. It has been very successful in finding and solving problems before they turn into crises."

"Companies that lack a clear vulnerability disclosure program are at increased risk should a security researcher find a vulnerability." - Megan Brown, Partner, Wiley Rein LLP

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, progress from the industry such as the VDP Framework recommended by the DoJ and Gartner's recent predictions that by 2022 crowdsourced security solutions will be employed by more than 50% of enterprises, up from less than 5% today leave us hopeful.

VDPs are designed to make it easy for any vulnerability to get into the right hands so it can be safely resolved. But until adoption of VDPs increases, vulnerabilities will continue to remain unreported. Nearly 1 **in 4 hackers have not reported a vulnerability that they found** because the company didn't have a channel to disclose it according to our 2018 Hacker Report. 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.



Vulnerability Disclosure Policy Statistics

61%

of startups valued at over $1 billion have a VDP. Companies born in the connected era are faster to adopt hacker-powered security.

5%

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

47%

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

20%

of conglomerates have vulnerability disclosure or bug bounty programs, including General Electric, Siemens, Honeywell International, ABB, Philips and others—up from 14% in 2017.

24%

of telecommunications companies have a known vulnerability disclosure program.

4%

of Financial Services companies named to the list have programs, including American Express, Citigroup, JPMorgan Chase, ING, Swedbank, Mastercard, Visa, TD Ameritrade, and others.

CUSTOMER SPOTLIGHT

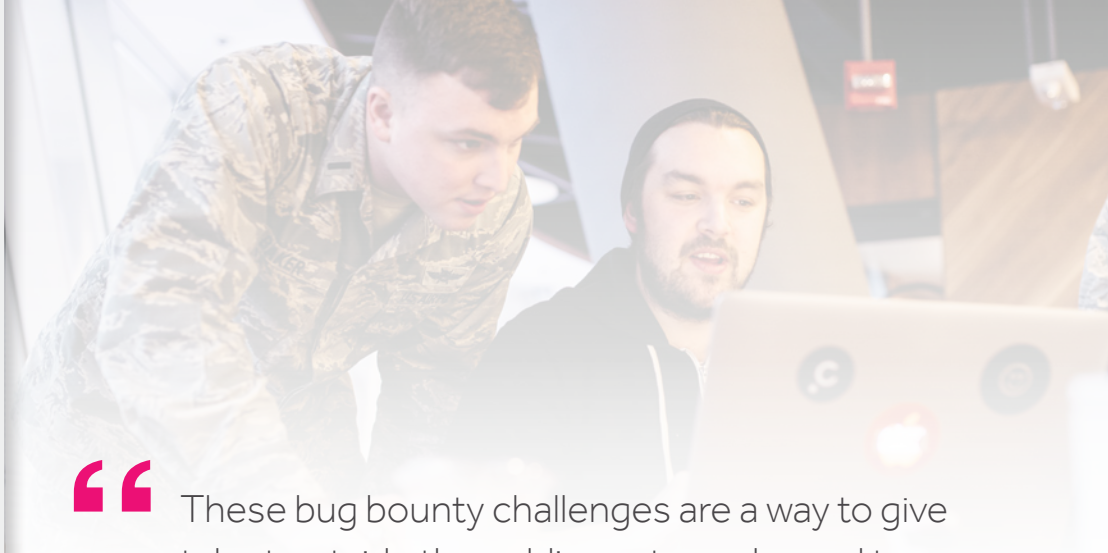
Department of Defense

In November 2016, following Hack the Pentagon bug bounty challenge, the U.S. Department of Defense launched its ongoing VDP. Since, the DoD has continued to run four more bug bounty challenges, Hack the Army, Hack the Air Force, Hack the Air Force 2.0, and Hack the DTS. To date, 5,000 vulnerabilities have been received in U.S. government systems and over $400,000 have been paid to ethical hackers in the process.

"Millions of government employees and contractors use and rely upon key enterprise systems every day," said Reina Staley, Chief of Staff at Defense Digital Service. "Any compromise of the system or the sensitive information it handles would be detrimental to our people and our mission. These bug bounty challenges are a way to give talent outside the public sector a channel to safely disclose security issues and get rewarded for these acts of patriotism."

Why do hackers choose to participate? "To improve the security of the world, one bug at a time," said Hack the Air Force winner and 18-year-old hacker Jack Cable (@cablej) to Chicago Magazine. "I love the challenge and impact."

"We continue to harden our attack surfaces based on findings of the previous challenge and will add lessons learned from this [second] round," said Air Force CISO Peter Kim. "This reinforces the work the Air Force is already doing to strengthen cyber defenses and has created meaningful relationships with skilled researchers that will last for years to come."



> "These bug bounty challenges are a way to give talent outside the public sector a channel to safely disclose security issues and get rewarded for these acts of patriotism.

REINA STALEY
Chief of Staff,
Defense Digital Service

VULNERABILITIES RESOLVED
3,000+

ORGANIZATION SIZE
400,000+

HACKERS REGISTERED TO PARTICIPATE IN HACK THE PENTAGON
1,410+

PRODUCT
HackerOne Challenge & Response

As of April 2018

Hacker Community Trends and Statistics

The 2018 Hacker Report, published by HackerOne in January, is the largest documented survey ever conducted of the ethical hacking community.

Here are some of the top highlights of the report, providing insights on the hacker mindset, statistics and growth metrics, where they're from, and what vulnerabilities they hunt.

200K+
TOTAL REGISTERED HACKERS

72K+
TOTAL VULNERABILITIES RESOLVED TO-DATE

$31M+
TOTAL BOUNTIES PAID

WHO ARE HACKERS AND WHY DO THEY HACK?

Youthful, curious, gifted professionals. Over 90% of hackers are under the age of 35 and 44% are IT professionals. **Bug bounties can be life changing for some hackers. The top hackers based in India earn 16x the median salary of a software engineer.**

Money remains a top reason for why bug bounty hackers hack, but it's fallen from first to fourth place compared to 2016. Above all, hackers are motivated by the opportunity to learn tips and techniques, with "to be challenged" and "to have fun" tied for second.

Nearly 58% of them are self-taught hackers. Despite 50% of hackers having studied computer science at an undergraduate or graduate level, and 26.4% studied computer science in high school or before, less than 5% have learned hacking skills in a classroom.

"**At the end of the day, we're all in this together**. We're trying to find stuff and fix issues. We're trying to help protect the world. That's what it comes down to. And I like to be a part of that," said Brett (@ziot).

On Average, Approximately How Many Hours Per Week Do You spend Hacking?

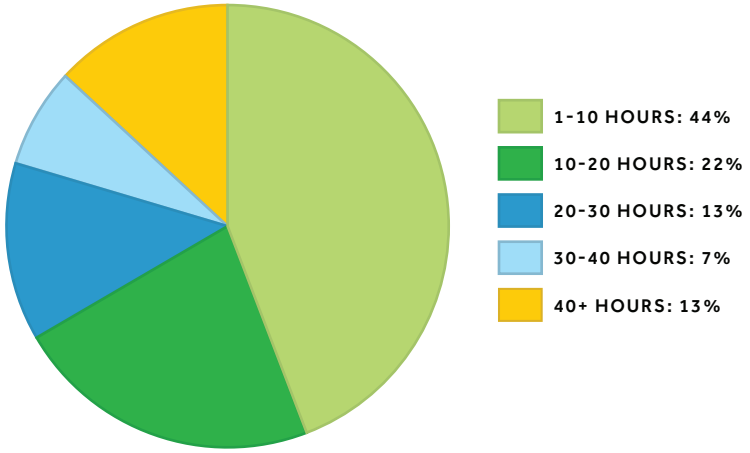


Figure 13

Why Do You Hack?

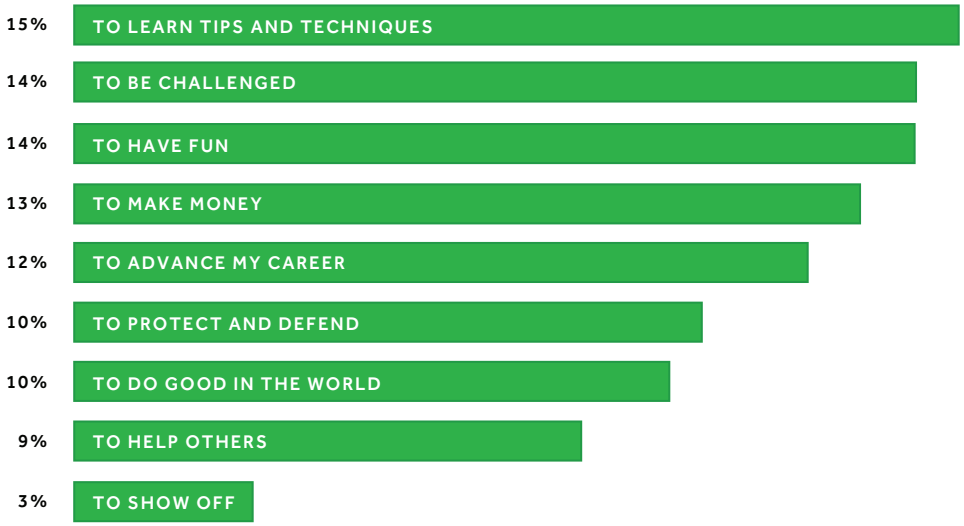


Figure 14

What's Your Age?

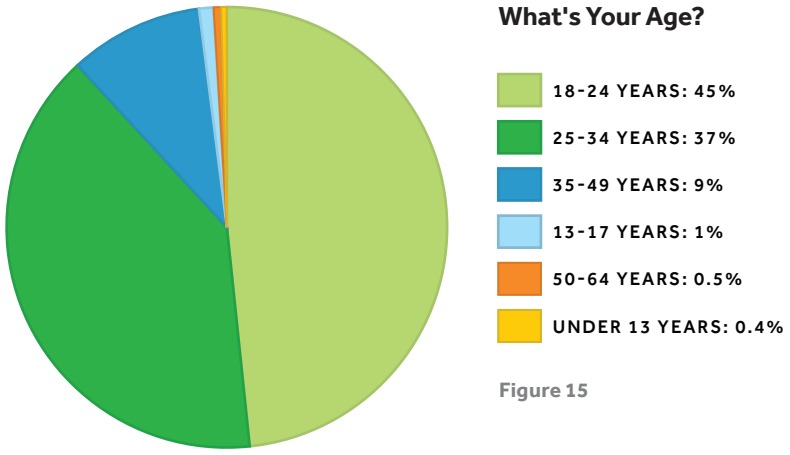


Figure 15

THE ECONOMICS OF BUG HUNTING

In the 2018 Hacker Report, we compared competitive salaries for an equivalent job to the bug bounty earnings of top performers in each country. Out of 40 countries we pulled economic salary data on, the average multiplier of the top performers in each of those regions was 2.7x. This means on average, top earning researchers make 2.7 times the median salary of a software engineer in their home country. Which country had the highest multiplier for 2017? India with a multiplier of 16x the median salary of a local software engineer. Hunting bugs is potentially 16x more lucrative than an alternative job as a software engineer. Now that's incentive to hack and hack a lot.

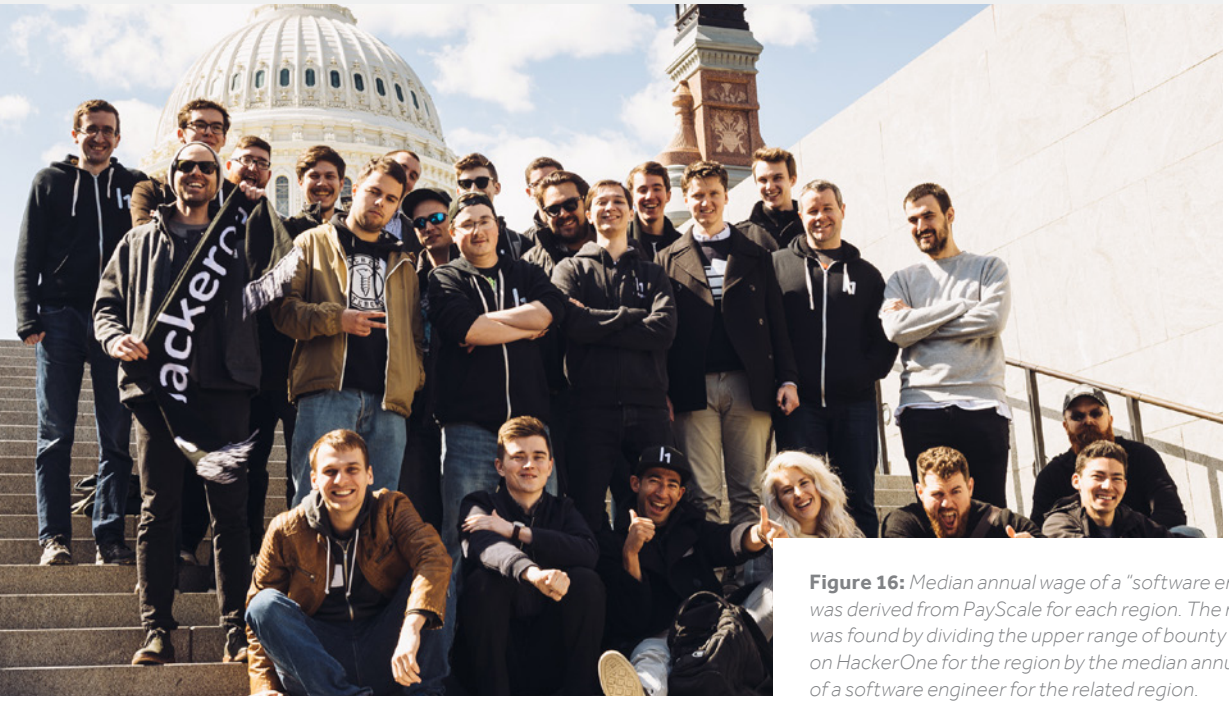


Figure 16: *Median annual wage of a "software engineer" was derived from PayScale for each region. The multiplier was found by dividing the upper range of bounty earners on HackerOne for the region by the median annual wage of a software engineer for the related region.*

Bug Bounty vs. Salary

	MULTIPLIER
India	16
Argentina	15.6
Egypt	8.1
Hong Kong	7.6
Philippines	5.4
Latvia	5.2
Pakistan	4.3
Morocco	3.7
China	3.7
Belgium	2.7
Australia	2.7
Poland	2.6
Canada	2.5
United States of America	2.4
Sweden	2.2
Bangladesh	1.8
Germany	1.8
Italy	1.7
Netherlands	1.7
Israel	1.6
Croatia	1.5
Czech Republic	1.5
Spain	1.5
Romania	1.2
Saudi Arabia	1.2

Hacker Quotes

"Since bug bounty is booming nowadays, competition between hackers is increasing. So, have some patience when you are first starting, and keep improving your recon skills. You have Internet, you have all the resources- keep reading from others' blogs and disclosed practical reports on HackerOne. Patience and better reporting is the KEY."

"I've always had somewhat of a mindset for security, even before I knew anything about computer science - growing up, my brain was constantly racing to figure out systems in order to find loopholes and workarounds that I could slip through."

"I jump around different programs. I've been acknowledged by Google, Yahoo, Uber, and most recently the U.S. Air Force for participating in the Hack the Air Force program...I was drawn to [DoD] programs because they offered a unique chance to disclose vulnerabilities in the U.S. government's systems. It's been great to see hackers help improve the Air Force's security and be recognized for their efforts."

"Personally I hack because I really love to build stuff and I also love to break stuff...the best way to know how to build stuff is to know how you can break it."

"The most meaningful purchase I made with bounty money is actually a car. For a really long time it was just one car in our house of three, and I really don't come from a wealthy background. It was really an issue trying to find a way to get around for everyone's jobs, so when I got into bug bounty I said, I'm going to get a car that everyone can use and I think it really helped."

"I couldn't quit hacking, so I had to find a way to use it to help companies protect themselves and their customers. I wanted to be part of the solution, and to make hacking a part of that."

"I absolutely love working on Burp Suite precisely because so many people use it. Just seeing when I have an idea for a scanning technique and I put it in the scanner and then a couple of months later I'll see publicly disclosed reports on HackerOne that were clearly found by Burp and that's the best feeling. Knowing that I can take a class of bug that's largely overlooked and just stomp on it is awesome."

"At the end of the day, we're all in this together. We're trying to find stuff and fix issues. We're trying to help protect the world. That's what it comes down to. And I like to be a part of that."

HACKER EDUCATION

According to Forrester Research Inc., around 1.8 million cybersecurity jobs will go unfilled by 2022, and 25% of security decision makers said lack of staff and the scarcity of security employees are to blame. While the hacker community is growing, less than 5% have learned hacking skills in a classroom and 25% are currently full-time students. A consistent theme every hacker has in common: curiosity and the thirst to learn. To train future cybersecurity leaders, the broader security community needs to invest in education. In 2017, HackerOne continued to do just that. While there is still a lot of work to be done, here are some highlights of hacker education efforts and events over the past year.

hacker101

Hacker101 is an online web security course designed to educate the next generation of ethical hackers. Taught by HackerOne security researcher Cody Brocious, the material trains enthusiastic bug hunters the skills required to be successful. Initially launched in January, 2018 the material has been very well received with over 80,000 total video views and more than 9,000 stars on GitHub in just five months. More content is being released monthly. Visit www.hacker101.com to learn more.

HACKERONE

DAY OF SHECURITY

Sponsored by

HackerOne is a sponsor and partner in S(h)ecurity, a security event to bring together female engineers for a workshop on hacking and cybersecurity.

Berkeley
UNIVERSITY OF CALIFORNIA

Hacking for college credit? Yes! HackerOne collaborated with UC Berkeley to design curriculum for a class that helped future software developers learn how to break software as they are building it.

An ongoing partnership with Code.org was born, bringing middle school and high school students to HackerOne's U.S. live-hacking events. Combined, HackerOne has hosted over 200 kids at hacking workshops where students learn about cybersecurity and hacking through hands-on experience, get personal guidance by world-class hackers, and collaborate on solving capture the flag challenges.

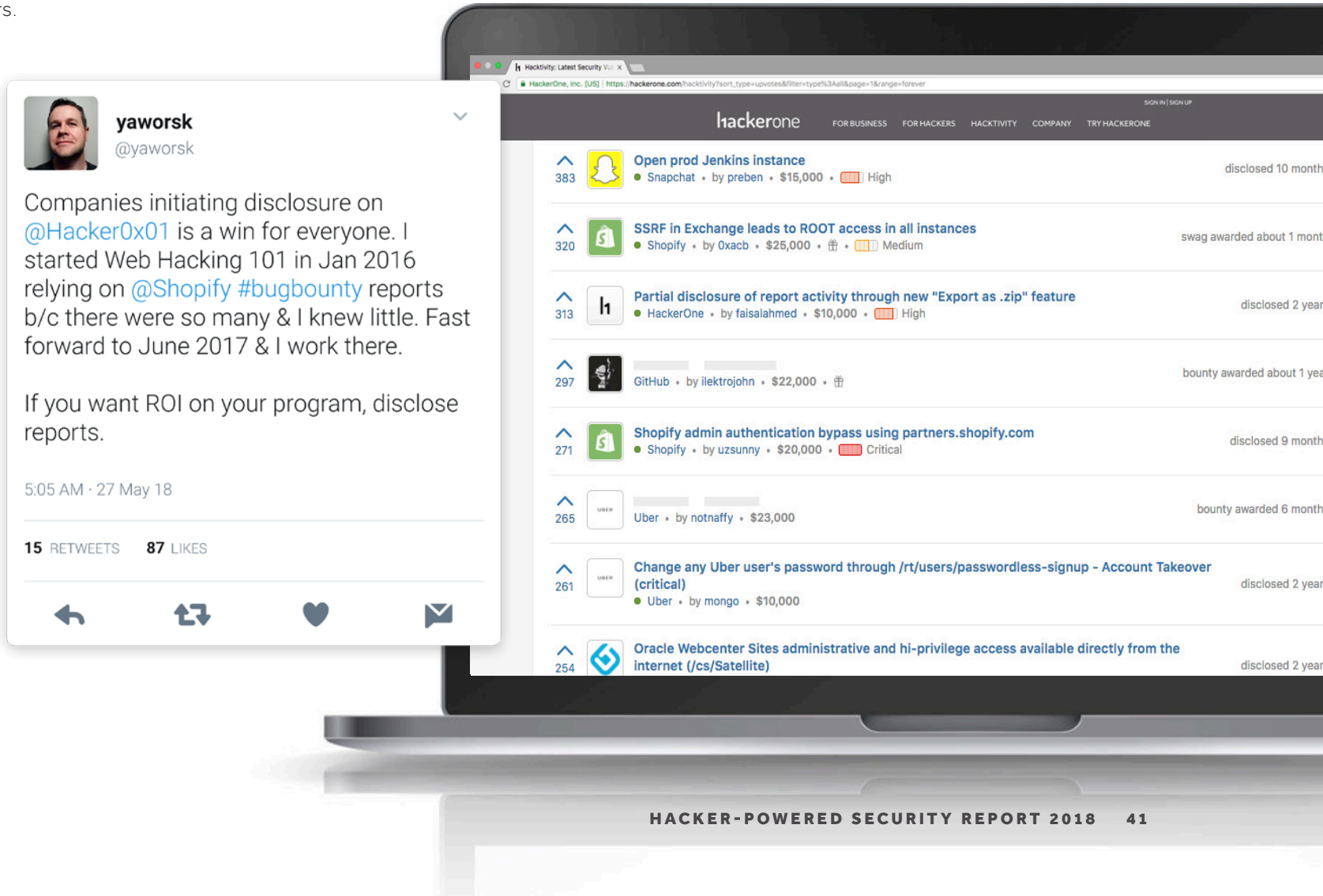
Zero Daily is a free infosec newsletter written and published by HackerOne. The daily news brief includes article links, top tweets, useful tools and fun and thought-provoking quotes on all things infosec with a focus on hacking, appsec and bug bounty topics. Reader Arne Swinnen says "[Zero Daily] is a great recap of news I care about. I read it everyday." Subscribe to Zero Daily and join thousands of readers enjoying their infosec news along with their cup of joe every morning.

"This is one of the best events that I've been to for the kids. The swag was great, the food was delicious, and the kids were so into it. Meeting people that are in the business is really important because it's something that they can relate to."

JENNIE LYONS
Computer Science Specialist, SFUSD

The Hacktivity Feed

The Hacktivity feed continues to be a resource for hackers to learn from their peers. Of note, in total, over 6,200 reports have been disclosed on HackerOne's hacktivity. These disclosed vulnerability reports are an invaluable learning tool for hackers, and a simple disclosure mechanism for HackerOne customers.



LIVE HACKING EVENTS

Picture the world's largest and most exciting one-day live penetration test where hackers collaborate and mingle with world-class security teams. Live hacking events bring the community together like never before. It's where community, camaraderie, and collaboration are exhibited in spades. It's where friends become family.

For a customer, a live hacking event increases engagement, builds relationships with top hackers, provides an opportunity to test new scope, and helps security teams and hackers work better together. For hackers, live events help them better understand what security teams value most, build relationships with security teams and other hackers, and provide unique opportunities to hack new scope and earn more cash.

In the past year, HackerOne hosted live hacking events in seven cities: Las Vegas (H1-702), New York City (H1-212), Goa, India (H1-91832), Washington DC (H1-202), San Francisco (H1-415), Amsterdam (H1-3120), and London (H1-4420). For each event, we partner with our customers to fly out 25 to 40 (sometimes over 50!) of the top members of our community from across the globe to participate.

Over 1 million in bounty cash has been awarded at these events, with Oath even paying out over $400K in one day in April 2018 at H1-415. These events bring together some of the best talent with eager security teams to uncover vulnerabilities, boost payouts and harden attack surfaces. But probably the most exciting of all: personal relationships are forged that last a lifetime.

BRINGING THE COMMUNITY TOGETHER FOR GLOBAL LIVE HACKING EVENTS

LAS VEGAS		JULY 2017
NEW YORK		DECEMBER 2017
GOA, INDIA		FEBRUARY 2018
WASHINGTON DC		MARCH 2018
SAN FRANCISCO		APRIL 2018
AMSTERDAM		MAY 2018
LONDON		JUNE 2018

Security@ Conference

In October 2017, HackerOne hosted the first-ever hacker-powered security conference, Security@ San Francisco. Over 250 security leaders, influencers, and hackers from over 150 organizations gathered to discuss everything from VDP best practices, to hacker-powered pen tests, to private and public bug bounties, and hacker motivations.

Speakers included world renowned hacker Samy Kamkar, Natalie Silvanovich from Google Project Zero, Wiley Rein, LLP lawyer Matthew J. Gardner, a panel of the world's top hackers, and security executives from U.S. General Services Administration, Defense Digital Service, Twine (John Hancock), Coinbase, Lending Club, General Motors, and Auto-ISAC.

Watch all the Security@ content for free, including Samy's keynote. Natalie's "attack surface reduction" masterpiece and more.

The event covered topics including opening up the government to hackers, the technical interconnection of bug hunting and reducing attack surfaces at the development level, the legal implications and considerations when inviting hackers into your security ecosystem, hacker motives and loyalty, how hackers fit into the financial sector and related regulations, and how the automotive industry is opening its arms to hackers in the wake of connected and autonomous vehicles.

Closing Thoughts

We wish to thank the tens of thousands of hackers and thousands of organizations who have produced the data for this report by being active users and promoters of hacker-powered security. When we all work together, cyber threats can be thwarted. Together we hit harder!

Methodology and Sources

Findings in this report were collected from the HackerOne platform using HackerOne's proprietary data based on over 1,000 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 one that does not have a 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 2018 Hacker Report: The report was based on over 1,700 responses to the 2017 HackerOne Community Survey, including hackers who successfully reported one valid vulnerability, as indicated by the organization that received the vulnerability report.

ABOUT HACKERONE

HackerOne is the #1 hacker-powered security platform, helping organizations receive and resolve critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security partner. Organizations, including the U.S. Department of Defense, U.S. General Service Administration, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, and the CERT Coordination Center trust HackerOne to find critical software vulnerabilities. HackerOne customers have resolved over 72,000 vulnerabilities and awarded over $31M in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York, and the Netherlands.