hackerone

THE HACKER-POWERED SECURITY REPORT 2017

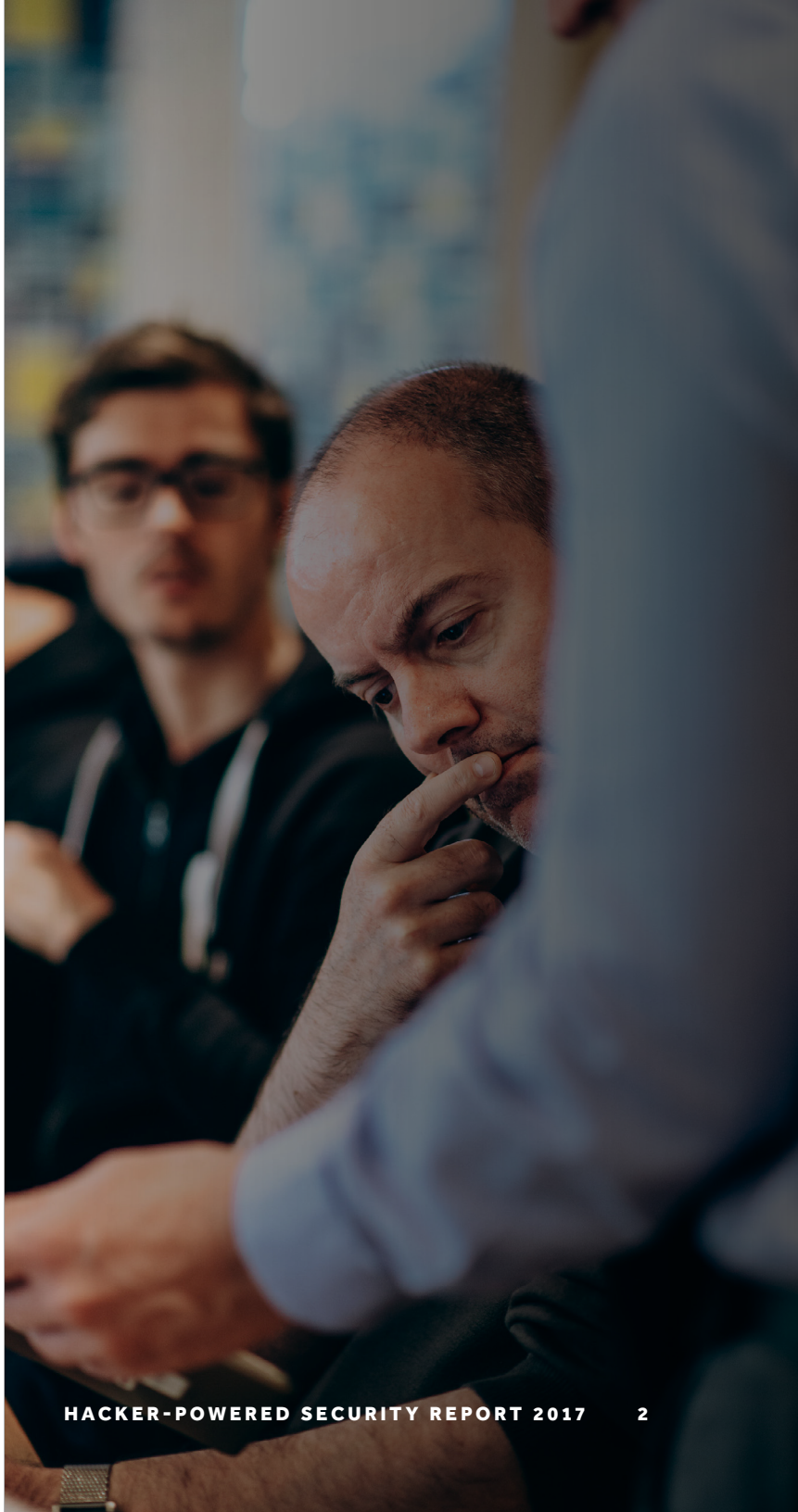
HackerOne's benchmark study on the hacker-powered security ecosystem

Executive Summary

Hacker-Powered Security: a report drawn from 800+ programs and nearly 50,000 resolved security vulnerabilities.

Bug bounty and hacker-powered security programs are becoming the norm, used by organizations as diverse as Facebook and the U.S. government. Forty-one percent of bug bounty programs were from industries other than technology in 2016. Top companies are rewarding hackers up to $900,000 a year in bounties and bounty rewards on average have increased 16 percent for critical issues since 2015. Despite bug bounty program adoption and increased reward competitiveness, vulnerability disclosure programs still lag behind. Ninety-four percent of the Forbes Global 2000 companies do not have policies.

It's time to give security teams the tools they need to keep up with ever-faster development. This report examines the broadest platform data set available and explains why organizations like General Motors, Starbucks, Uber, the U.S. Department of Defense, Lufthansa, and Nintendo have embraced continuous, hacker-powered security.



Contents

Introduction

Security experts are in high demand as hundreds of millions of lines of new code are deployed each day. Hacker-powered security provides a way to identify high-value vulnerabilities faster, leveraging the creativity of the world's largest ethical hacker community.

"We know for a fact that sending a wide variety of hackers into a wide environment wil result in something meaningful. It is a fact. We cannot hire every amazing hacker and have them come work for us, but we can do these crowdsourced bug bounties."

- Chris Lynch, Director, U.S. Department of Defense, Defense Digital Services

Our data reveals that adoption of bug bounty programs has moved beyond the technology industry. Governments, multinational financial services, media and entertainment organizations, and global retail providers are partnering with hackers worldwide to help protect their digital assets.

The earliest recorded bug bounty program dates back to 1983 with Hunter & Ready, Inc.'s "Get a bug if you find a bug" campaign. This model was later reintroduced by Netscape in 1995 and perfected by Microsoft, Google, Facebook, and Mozilla. Today, software is at the center of virtually every industry and societal function. Criminals are getting better at exploiting vulnerabilities, harming consumers and industry trust, and costing hundreds of millions of dollars in damage. In mid-May 2017, the massive WannaCry ransome attack affected hundreds of organizations worldwide, including the United Kingdom's National Health Service and Spain's Telefonica. The estimated cost from computer downtime from the attack: over $8 billion. In 2016, the average cost of a data breach exceeded $4 million, and almost half of all breaches were caused by malicious or criminal attacks, according to the Ponemon Institute.

Hacker-powered security has proven to be an essential safeguard against criminal attacks.

The first "bug" bounty program that paved the way for today's industry dates back to 1983 from operating system company Hunter & Ready, Inc.

HACKER-POWERED PROGRAMS DEFINED

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 defined in ISO standard 29147.

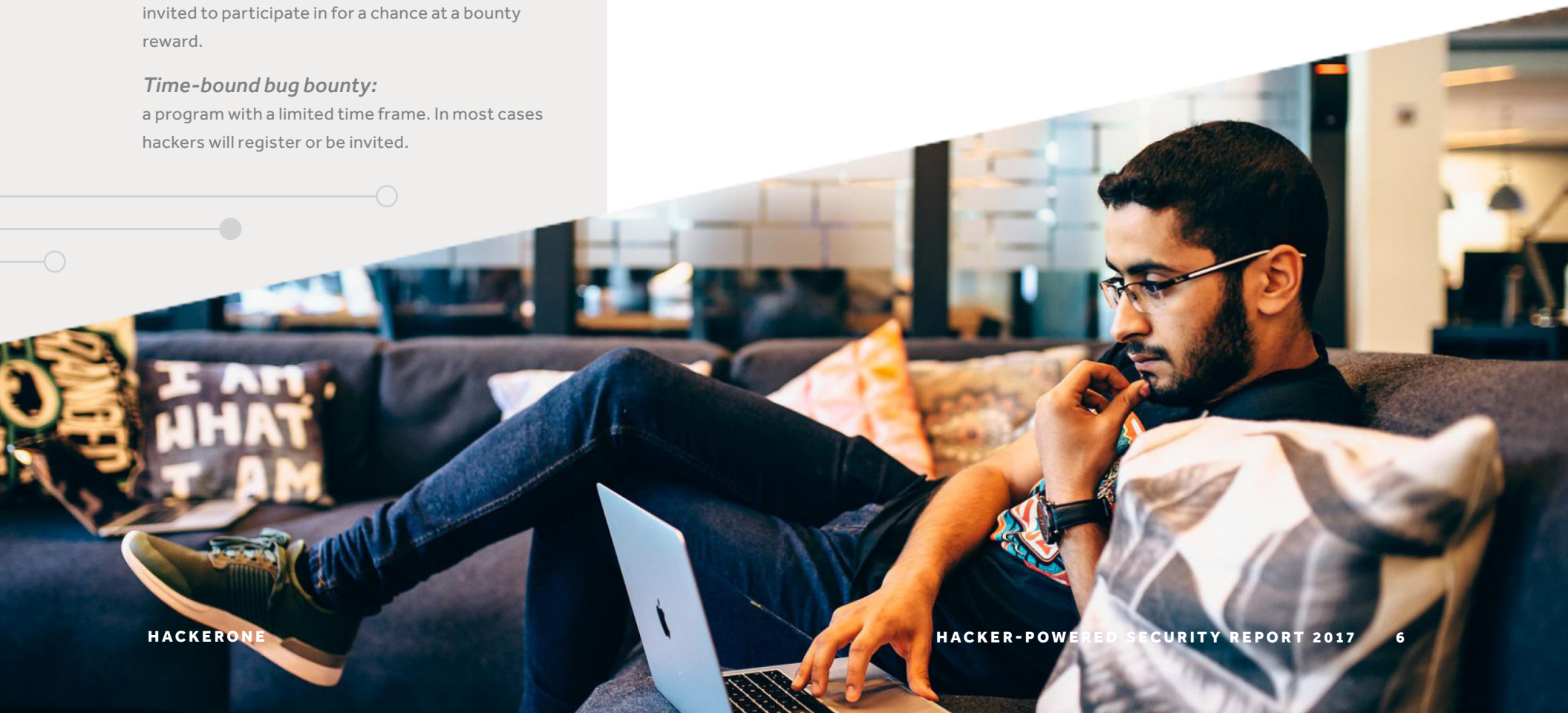
Bug bounty program:
an open program any hackers can participate in for a chance at a bounty reward.

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:
a program with a limited time frame. In most cases hackers will register or be invited.

What is hacker-powered security?

Hacker-powered security is any technique that utilizes the power of the external hacker community to find unknown security vulnerabilities in technology. 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.



Key Findings

This report examines the largest dataset of more than 800 hacker-powered security programs, as well as surveyed responses from individuals managing these hacker-powered programs and the hackers who participate. The report also analyzed vulnerability disclosure data from the world's 2,000 biggest publicly traded companies according to Forbes.

1. **Bug bounties aren't just for technology companies.** While over half of bug bounty programs launched in 2016 are for technology companies, 41 percent are from other industries. Governments, media and entertainment, financial services and banking, and ecommerce and retail industries all showed significant growth year over year.

2. **Customers security response efficiency is improving.** The average time to first response for security issues was 6 days in 2017, compared to 7 days in 2016. Ecommerce and retail organizations fixed security issues in four weeks, the fastest on average.

3. **Responsive programs attract top hackers.** Programs that are the fastest at acknowledging, validating, and resolving submitted vulnerabilities are the most attractive to hackers. Loyalty matters — repeat hackers are to thank for the majority of valid reports.

4. **Bounty payments are increasing.** The average bounty paid to hackers for a critical vulnerability was $1,923 in 2017, compared to $1,624 in 2015 — an increase of 16 percent. The top performing bug bounty programs award hackers an average of $50,000 a month, with some paying nearly $900,000 a year.

5. **Vulnerability disclosure policies.** Despite increased bug bounty program adoption and recommendations from federal agencies, 94 percent of the top publicly-traded companies still do not have known vulnerability disclosure policies — unchanged from 2015.

6. **Security vulnerabilities worry companies the most.** Seventy-three percent of surveyed customers said they are concerned about unknown security vulnerabilities being exploited, while 52 percent said they also fear customer data and intellectual property theft.

Bug Bounty Program Growth by Industry

Forty-one percent of new bug bounty programs launched between January 2016 to 2017 came from industries beyond technology. Within technology there was an increase in the number of Internet of Things (IoT) and smart home programs launched, as well as open-source projects. While technology companies still represent the majority (59%), growing verticals include financial services and banking (10% of new programs), followed by media and entertainment (10%) retail and ecommerce (6%), and travel and hospitality (3%).

In April 2016, the first bug bounty program in the history of the U.S. federal government launched with the Department of Defense's Hack the Pentagon followed by the U.S. Army, U.S. Air Force, GSA's Technology Transformation Service, and the Internal Revenue Service. In late May 2017, U.S. Senators introduced a bill to establish a federal bug bounty program in the Department of Homeland Security. The U.K. government also announced a vulnerability disclosure policy pilot. These actions suggest that **hacker-powered programs are increasingly viewed as vital for securing digital assets for the public sector.**

With 76 percent, ecommerce and retail had the most significant adoption rates year-over-year. Gaming came in second with 75 percent. This was measured as overall growth in hacker-powered security adoption from January 1, 2016 to May 31, 2017.

There has been a 46 percent increase year over year in publicly disclosed vulnerability reports. These disclosed vulnerability reports in many cases are available in their entirety for anyone to learn from.

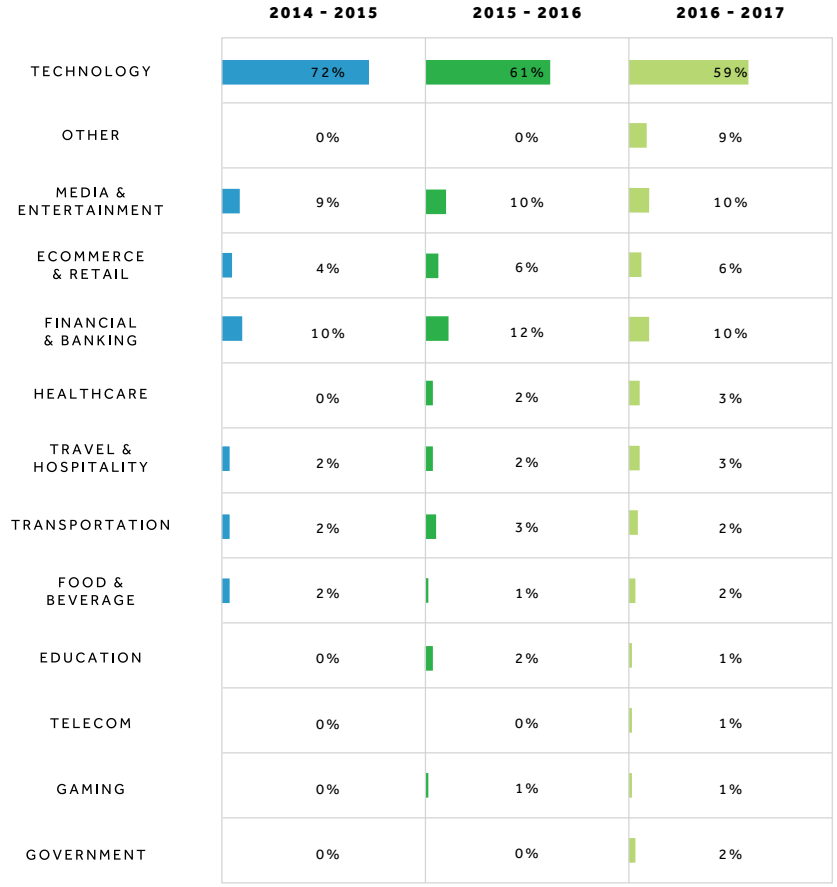


Figure 1: *Industries that launched programs from the overall share of programs, year over year.*

Vulnerabilities by Industry

Through May 2017, nearly 50,000 security vulnerabilities were resolved by customers on HackerOne, over 20,000 in 2016 alone.

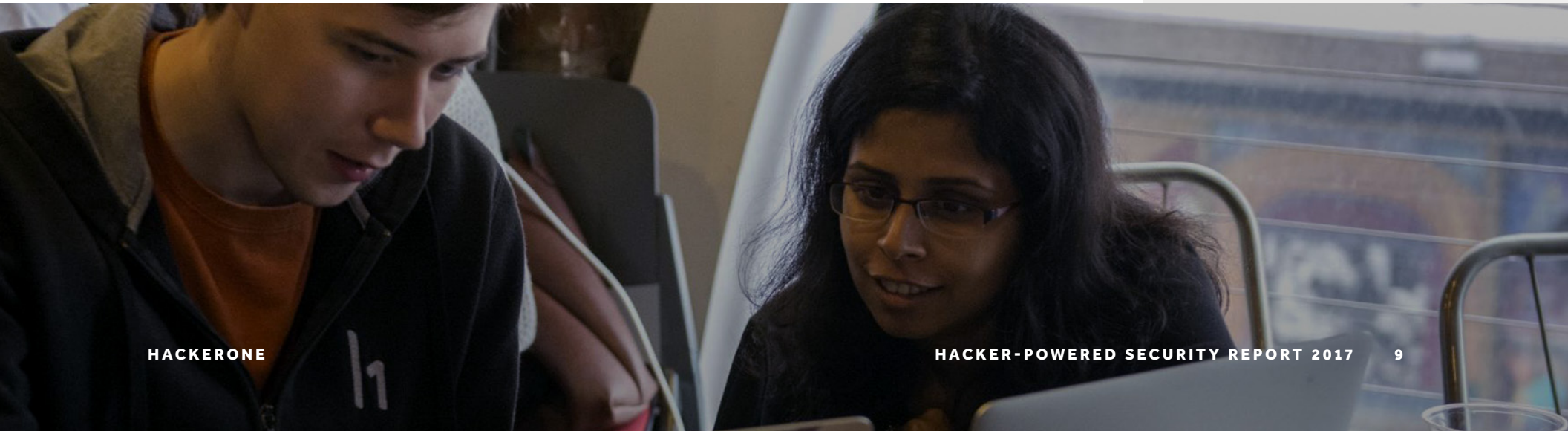
In all industries except for financial services and banking, cross-site scripting (XSS, CWE-79) was the most common vulnerability type discovered by hackers using the HackerOne platform. For financial services and banking, the most common vulnerability was improper authentication (CWE-287). Healthcare programs have a notably high percentage of SQL injection vulnerabilities (6%) compared to other industries during this time period.

Introducing a Cross-Site Scripting (XSS) vulnerability is easy. For example, if any user input is used and the HTML page is not sanitized, it is likely an XSS vulnerability. Modern browsers like Google Chrome can also protect the end users against certain XSS vulnerabilities. It's also becoming more common for application developers to use front-end frameworks, like React, AngularJS, and Ember.js. Most of these frameworks are safe by default when it comes to XSS vulnerabilities, meaning as long as the framework practices are followed, they mitigate XSS vulnerabilities.

Like all vulnerabilities, XSS issues range in severity. A reflected XSS vulnerability on a site that doesn't authenticate users and/or exposes any sensitive information would likely be low severity. An XSS issue on a system that exposes significant confidential information is more severe on the other hand. Organizations working with hackers receive a range of XSS issues including low and high severity. At HackerOne, the severity of every security vulnerability is measured with Common Vulnerability Scoring System framework (CVSS) v3.0.

Financial services are often targeted by criminals. In 2016 over 200 million records were compromised in the financial services sector — a 937 percent increase year over year, according to IBM X-Force® Research.

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



VULNERABILITIES BY INDUSTRY

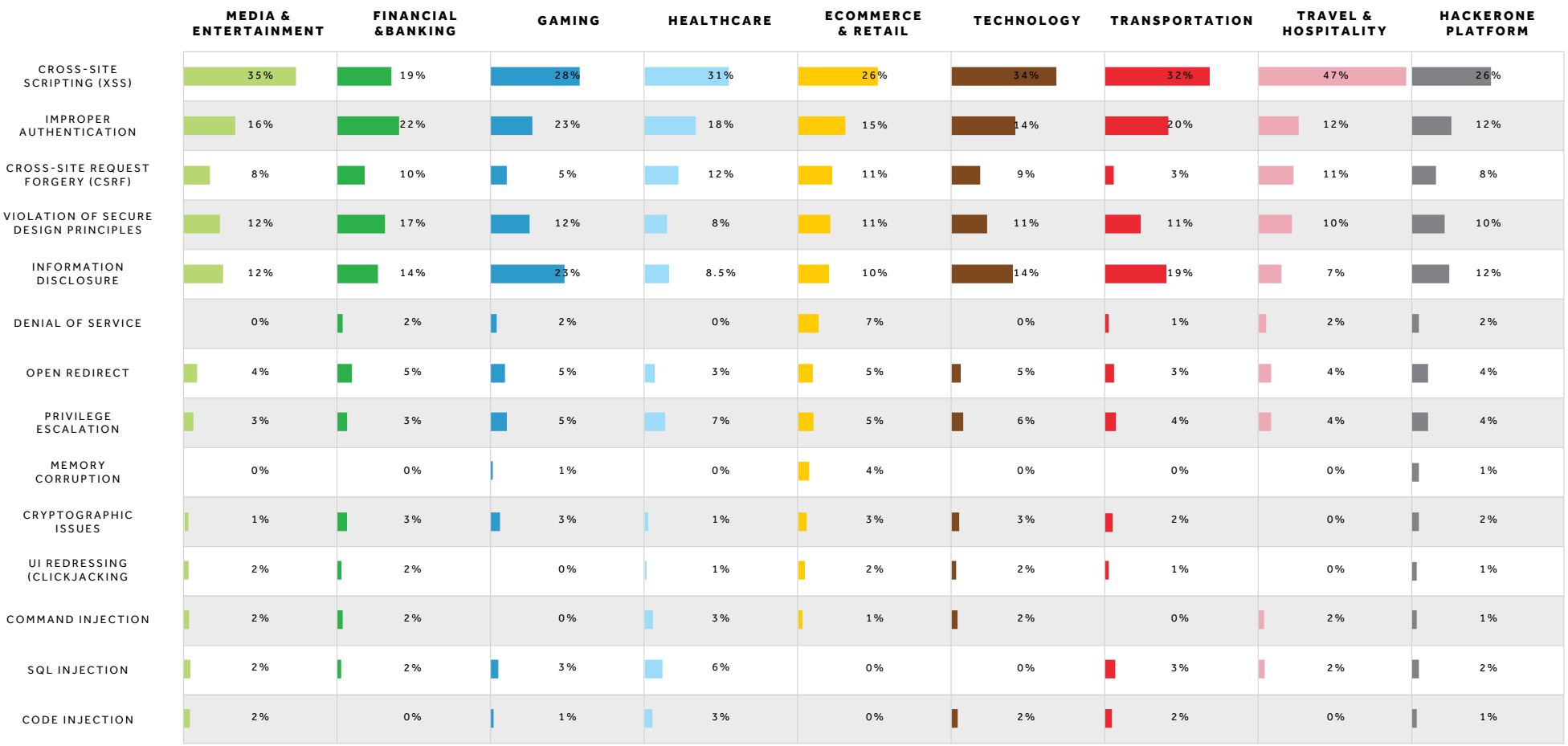


Figure 2: *Percentage of vulnerability type by industry from 2013 to May 2017.*

In March 2017 HackerOne updated its vulnerability taxonomy to include the industry-standard Common Weakness Enumeration (CWE). This taxonomy provides a much more complete and accurate description of a reported vulnerability, using language endorsed by the security community.

Time to Resolution

Seventy-seven percent of all bug bounty programs have their first vulnerability reported in the first 24 hours. 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 resolution for all programs. A speedy resolution not only helps protect the organization and its customers faster (by fixing the issue), it also helps attract hackers to the customer's program (by paying hackers faster).

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

RESOLUTION TIME MATTERS
It is easier and less expensive to fix vulnerabilities than to mitigate them.

GARTNER PREDICTS
Ninety-nine percent of vulnerabilities exploited through 2020 will continue to be known by security and IT professionals for at least one year.

Based on time to resolution data in the HackerOne platform, ecommerce and retail businesses are the fastest at resolving vulnerabilities, taking a total of 31 days on average. Education organizations are the next fastest, resolving vulnerabilities in 33 days on average. Certain industries resolve issues more slowly, particularly in highly regulated areas with complex software stacks and supply chains, such as telecommunications and government.

Now that's fast!
It took Slack's security team just five hours from when the report was filed to fix a cross-origin token vulnerability reported in February 2017.

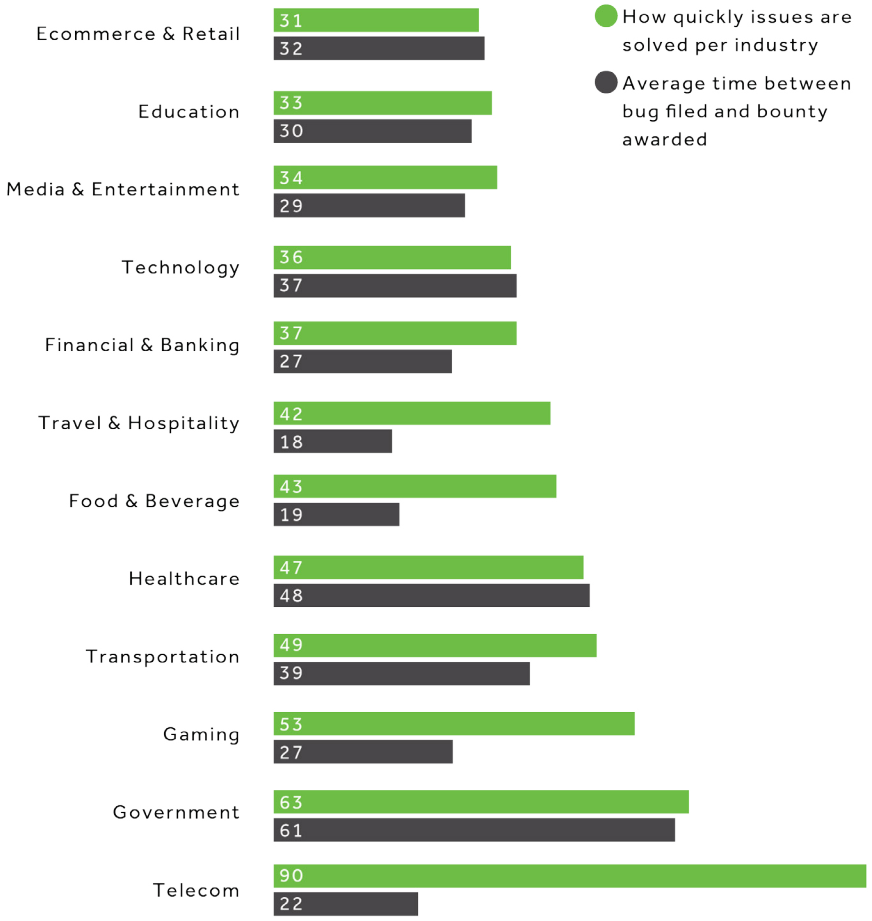
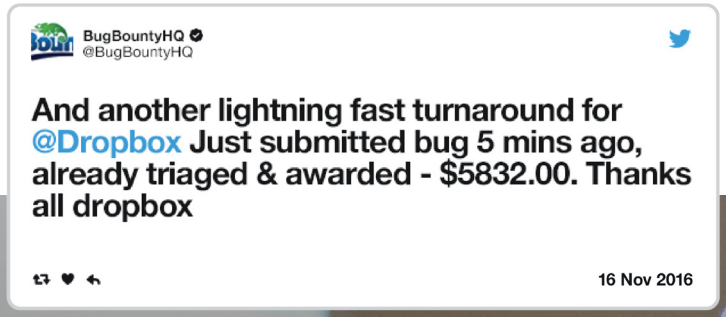


Figure 3: *Average number of days to resolution and to reward, measured from Jan 1, 2016 to May 31, 2017.*

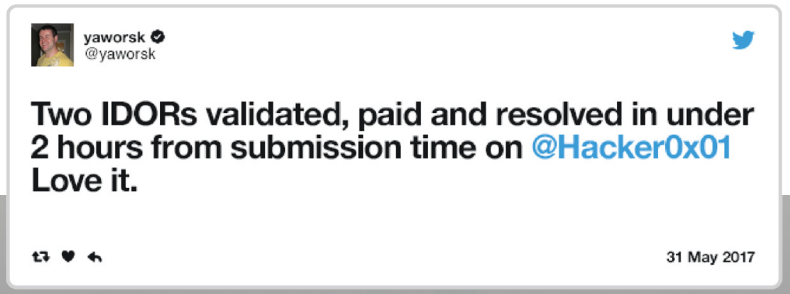
Another way to measure speed is to look at how quickly industries pay bounties once bugs or vulnerabilities are filed by hackers. Travel and hospitality businesses pay the fastest, 18 days after the report is submitted, on average, followed by food and beverage (19 days). Due to the unique way government programs are structured, government organizations take the longest to pay (61 days).

HackerOne data shows variability in which step of the process organizations pay bounties. About one out of every five will pay when the vulnerability is validated (18%), and half will pay when a vulnerability is resolved (48%) , and the remainder pay on a case-by-case basis (34%). Rewarding a hacker quickly for a severe vulnerability can be a reflection of its priority and a signal to the researcher of its importance to the organization.

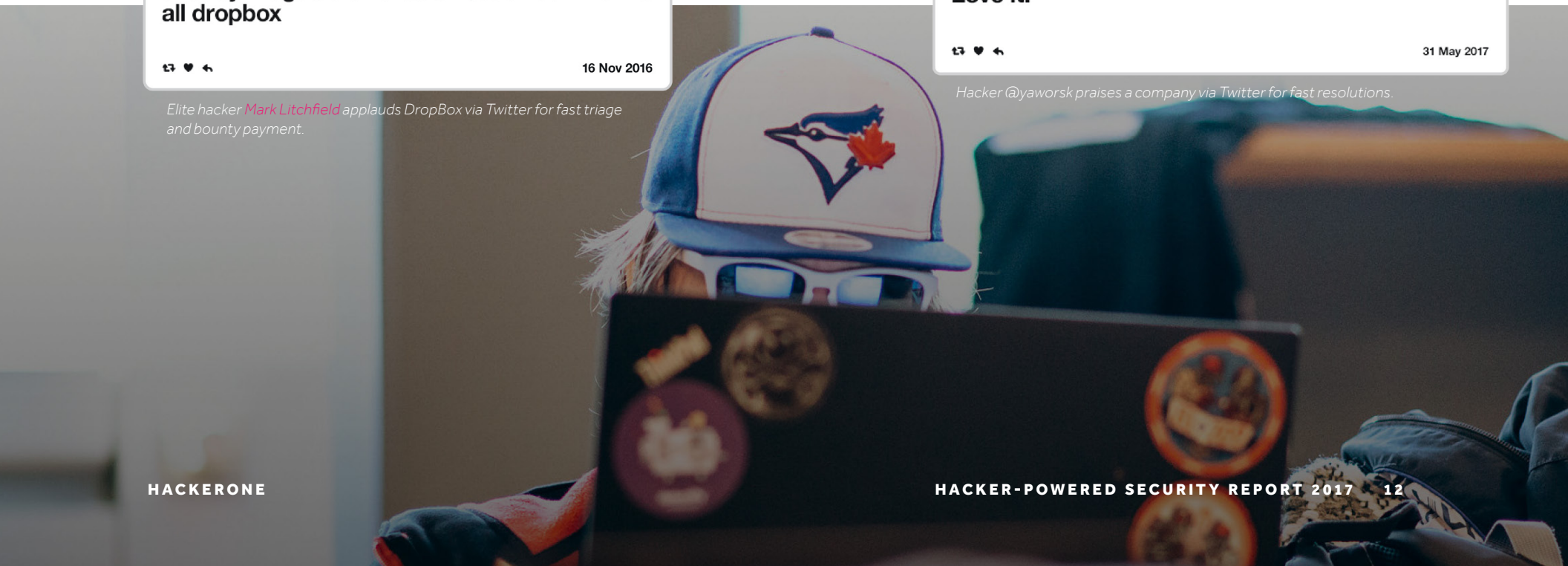
A hacker participating in the U.S. Air Force bug bounty program shares on Twitter that the response time exceeded his expectations.



Elite hacker Mark Litchfield applauds DropBox via Twitter for fast triage and bounty payment.



Hacker @yaworsk praises a company via Twitter for fast resolutions.



Bounties by Severity

Bug bounty programs on the HackerOne platform that reward $15,000 on average for critical vulnerabilities are in the top 1% of reward competitiveness. Those programs reward higher bounties than 99 percent of the programs on HackerOne. In comparison 60% of organizations on the platform reward $1,000 on average for critical vulnerabilities.

Bug bounty programs will pay average 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 on average, than in an organization that pays $1,000 on average.

Hardening your attack surface and increasing reward competitiveness takes time and sustained effort. For example, Google Chrome steadily increased their top bounty from $3,000 to $100,000 over the course of more than five years. **Bug bounty programs offering bounties in the top 1 percent get there by continuously working with hackers to improve security.**

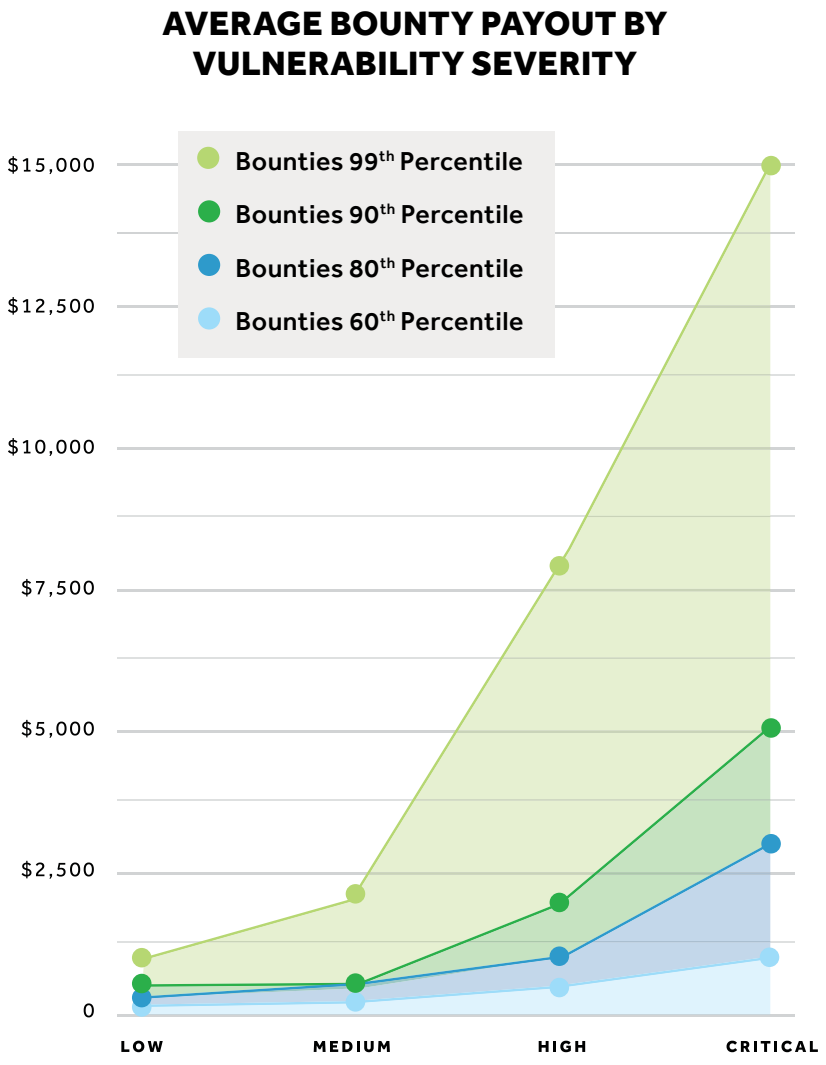


Figure 4: *Bug bounty reward competitiveness for critical vulnerabilities from January 2016 to 2017. Organizations in the 99th percentile, rewarding $15,000 on average, are rewarding bounties higher on average than 99 percent of the programs on HackerOne.*

Bounty Trends

Through May 2017, organizations have awarded hackers over $17 million in bounties on HackerOne, and over $7 million awarded in 2016 alone.

As more organizations launch bug bounty programs and compete for hacker talent, payouts are on the rise. In March 2017, Google increased their bounty award 50 percent, Microsoft doubled their top bounty award and Intel offered $30,000 for critical vulnerabilities. Offering competitive bounty awards help attract top hackers.

The highest amount paid for a single critical vulnerability on the platform was $30,000 by a technology company — an amount that has been awarded multiple times. In the last year, gaming, ecommerce and retail, and media and entertainment programs each awarded a $20,000 bounty to hackers for a critical vulnerability. **In the past 12 months, 88 individual bounties were over $10,000.**

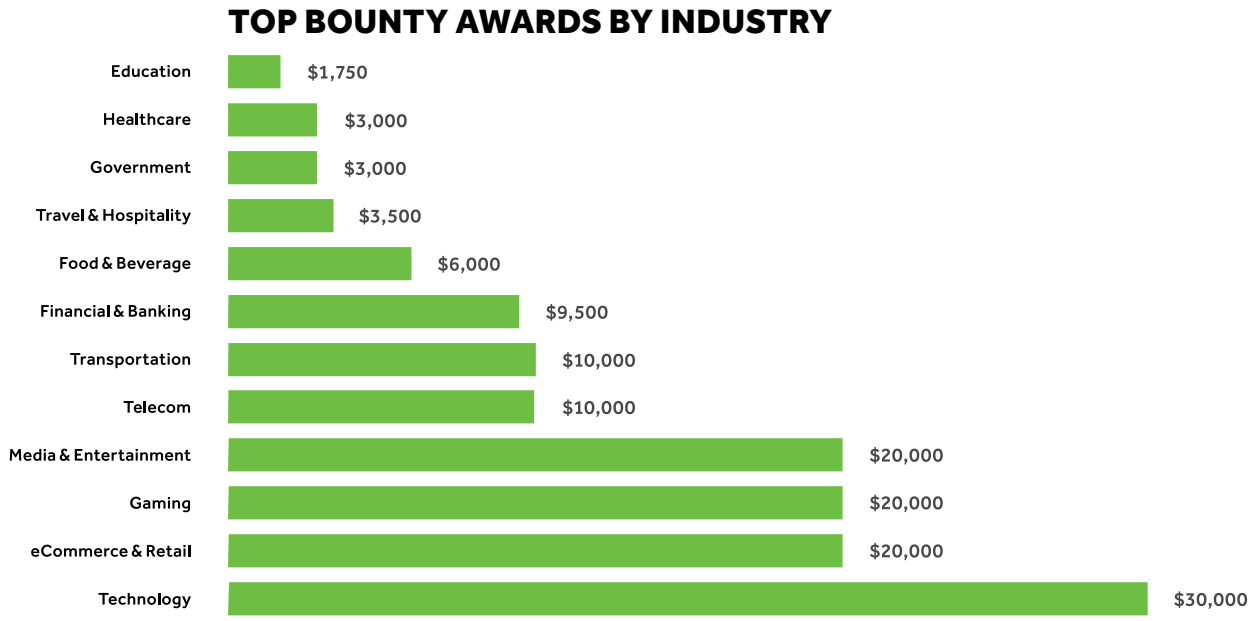


Figure 5: *When looking at total bounty awards by industry from 2013 through May 2017, companies from technology top the list, having awarded hackers over $9 million. Gaming is second, with over $1.5 million, followed by ecommerce and retail, and transportation at $1 million each.*

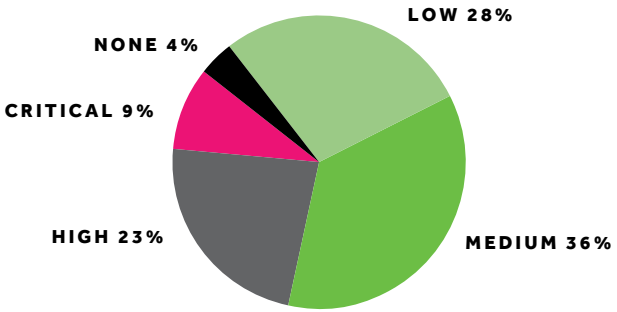
ATTRACTING TOP HACKER TALENT

Companies know that paying higher bounties helps attract and retain top hackers working on your program. In 2016, Shopify awarded $365,000 in one day; GitHub offered bounty "bonus rewards" of up to $12,000 for standout bug reports, and Uber launched a loyalty program that rewards repeat hackers with cash bonuses.

Bounty Trends

Looking at bounty averages by industry for critical issues, the highest average payments come from transportation ($4,491), followed by gaming ($3,583). Through May 2017, the average bounty for a critical issue paid to hackers on the HackerOne Platform was $1,923. For all vulnerabilities reported of any severity, the average bounty payout was $467.

Vulnerabilities submitted by hackers are ranked either low, medium, high or critical as part of the scoring process. Averages are from May 2016 to May 2017. HackerOne uses the Common Vulnerability Scoring System (CVSS) 3.0 calculator to assign severity.



VULNERABILITIES BY SEVERITY

Figure 6: *Percentage of vulnerability type by severity Jan 2016 to May 2017.*

AVERAGE BOUNTY PAYOUT PER INDUSTRY FOR CRITICAL VULNERABILITIES

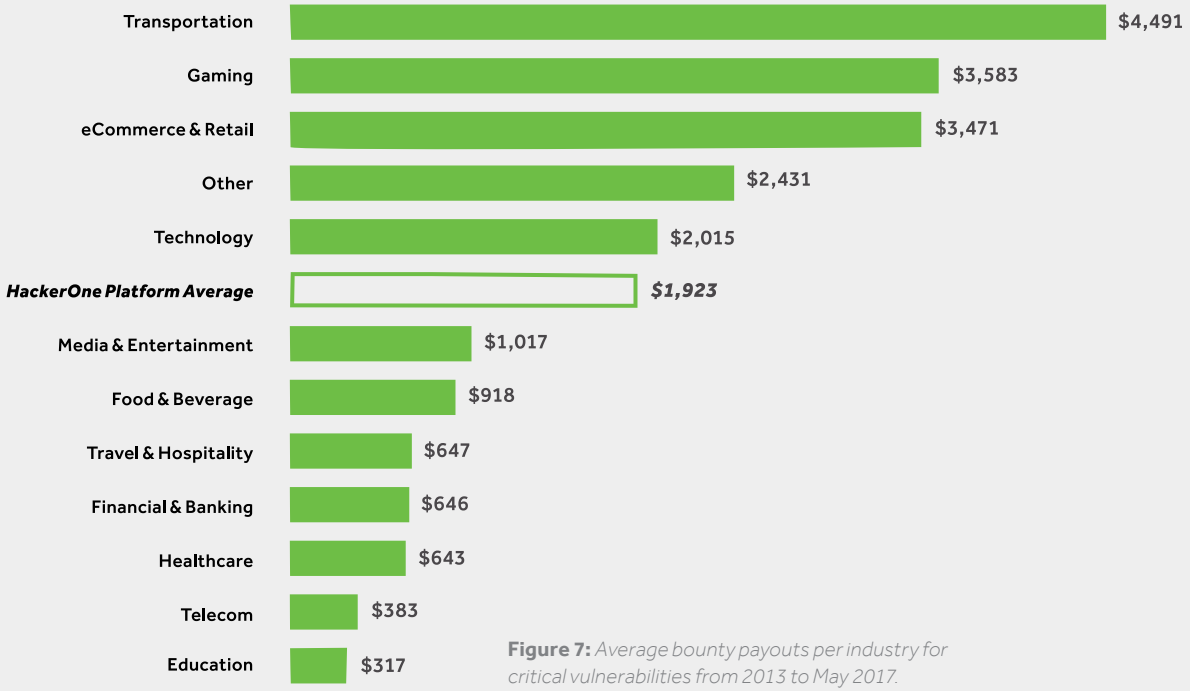


Figure 7: *Average bounty payouts per industry for critical vulnerabilities from 2013 to May 2017.*

TOTAL BOUNTY PAYOUT PER INDUSTRY

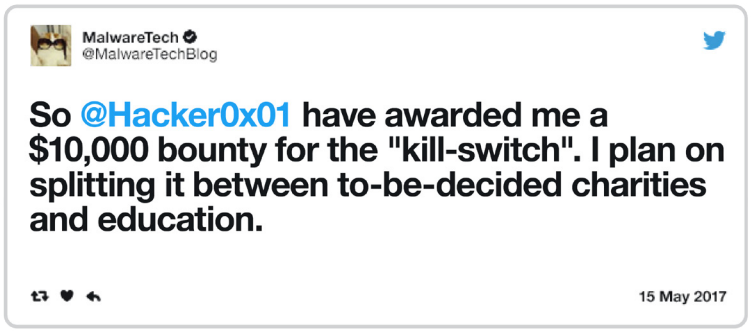
Technology	$9,003,004
Gaming	$1,508,289
Ecommerce & Retail	$1,053,631
Transportation	$1,047,259
Media & Entertainment	$638,830
Financial & Banking	$506,176
Food & Beverage	$198,437
Travel & Hospitality	$189,886
Healthcare	$140,345
Government	$83,200
Education	$68,150
Telecom	$27,450

Figure 8: *Total bounty payouts per specified industries from 2013 to December 2016.*

HACKERS DONATING BOUNTIES TO CHARITY

Hackers are increasingly donating their bounties to charitable organizations. Since 2014, hackers have donated nearly $100,000 to charities including Doctors Without Borders, UNICEF, the Electronic Frontier Foundation, and the Freedom of the Press Foundation. From January 1 through May 2017, hackers elected to donate $39,450 in bounties. The best customer programs match the donations made by the hackers.

> Many hackers also offer their time to directly help charitable causes. One such group is Security Without Borders.

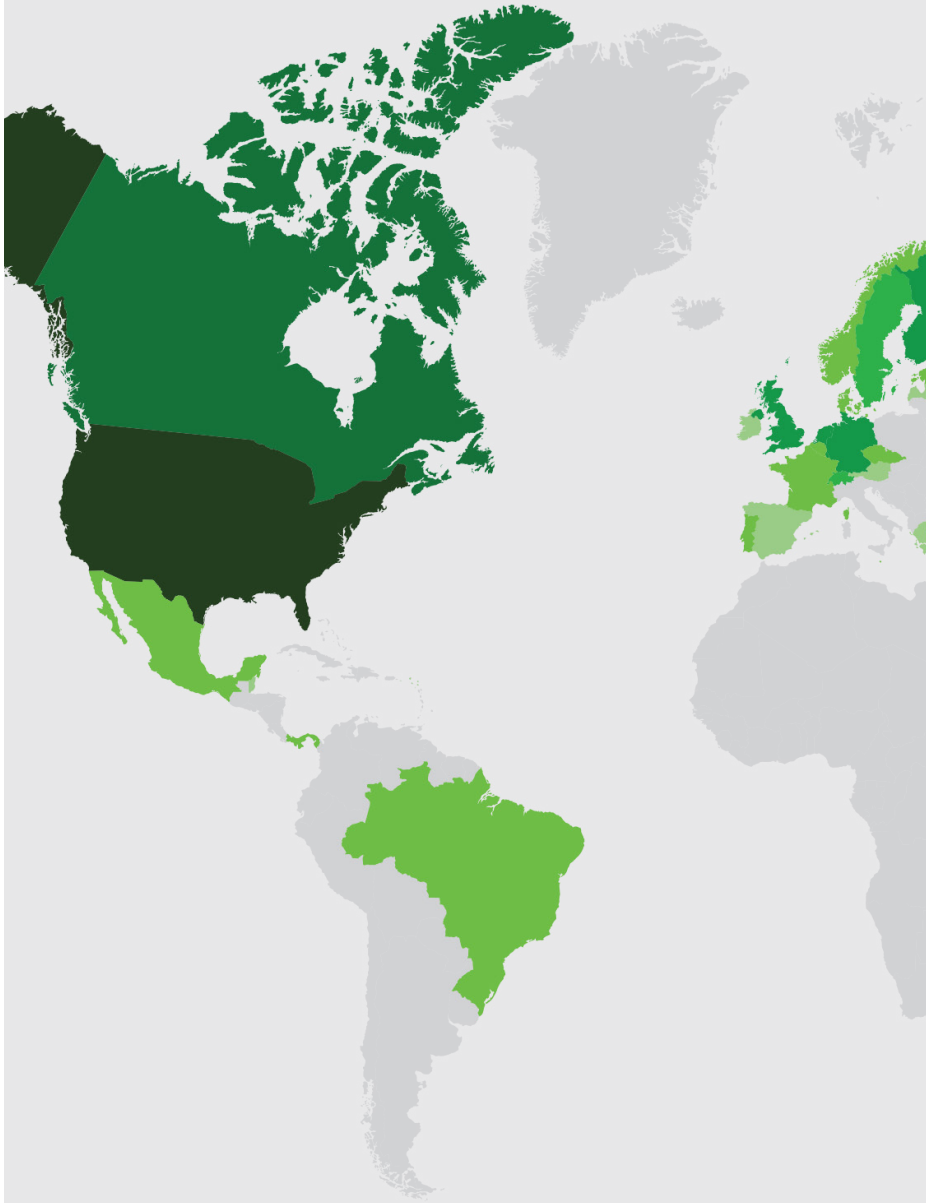


Hacker @MalwareTechBlog found the 'kill switch' for WannaCry malware that stopped it from infecting other computers. He was awarded a bounty for his contributions to making the internet safer.

Bounties by Geography

	WHERE HACKERS ARE EARNING BOUNTIES	LOCATION OF COMPANY PAYING BOUNTIES
United States of America	**$2,435,169**	**$6,945,487**
India	**$1,814,578**	$50
Australia	**$1,065,095**	**$24,801**
Russia	**$723,778**	**$137,634**
Sweden	**$633,701**	**$25,230**
United Kingdom	**$539,946**	**$159,306**
Argentina	**$506,672**	$0
Hong Kong	**$415,210**	$950
Germany	**$377,621**	**$116,811**
Pakistan	**$365,885**	$0
Canada	**$355,014**	**$662,915**
Morocco	**$273,688**	$0
Philippines	**$261,248**	$3,340
Netherlands	**$249,256**	**$167,745**
China	**$227,137**	$3,340
Luxembourg	$167,745	**$116,765**
Finland	$81,034	**$103,424**
Japan	$63,246	**$28,757**
Singapore	$48,964	**$47,761**
Switzerland	$23,004	**$89,473**
United Arab Emirates	$16,560	**$33,135**
Mexico	$2,700	**$9,920**

Figure 9: *Where hackers are earning the most dollars in total bounties, from April 2016 to April 2017. Where organizations are paying hackers the most dollars in total, from April 2016 to April 2017.*



HackerOne has awarded bounties in over 90 countries.

Public vs. Private Bug Bounty Programs

Private bug bounty programs make up 88 percent of all bug bounty programs on HackerOne and 92 percent of the bug bounty programs launched in 2016. The majority of public bug bounty programs are from technology (64%) followed by financial services and banking (11%) and media and entertainment (8%). In contrast, 100 percent of programs are private in the travel and hospitality, healthcare, insurance, aviation, and telecommunications industries.

While public programs made up only eight percent of HackerOne bug bounty launches in the past 12 months, public programs pay bounties and resolve issues at four times the rate of private programs.

PUBLIC BUG BOUNTY PROGRAMS RESOLVE 4X AS MANY VULNERABILITIES AS PRIVATE PROGRAMS.

Clear Signal:
Vulnerability reports closed as "resolved." This means the issue was a valid security bug that was fixed by the vulnerability response team.

Nominal Signal:
These reports are closed and 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.

HackerOne has the highest published Signal-To-Noise Ratio (SNR) in the industry. To read more, see "Improving Signal Over 10K bugs"

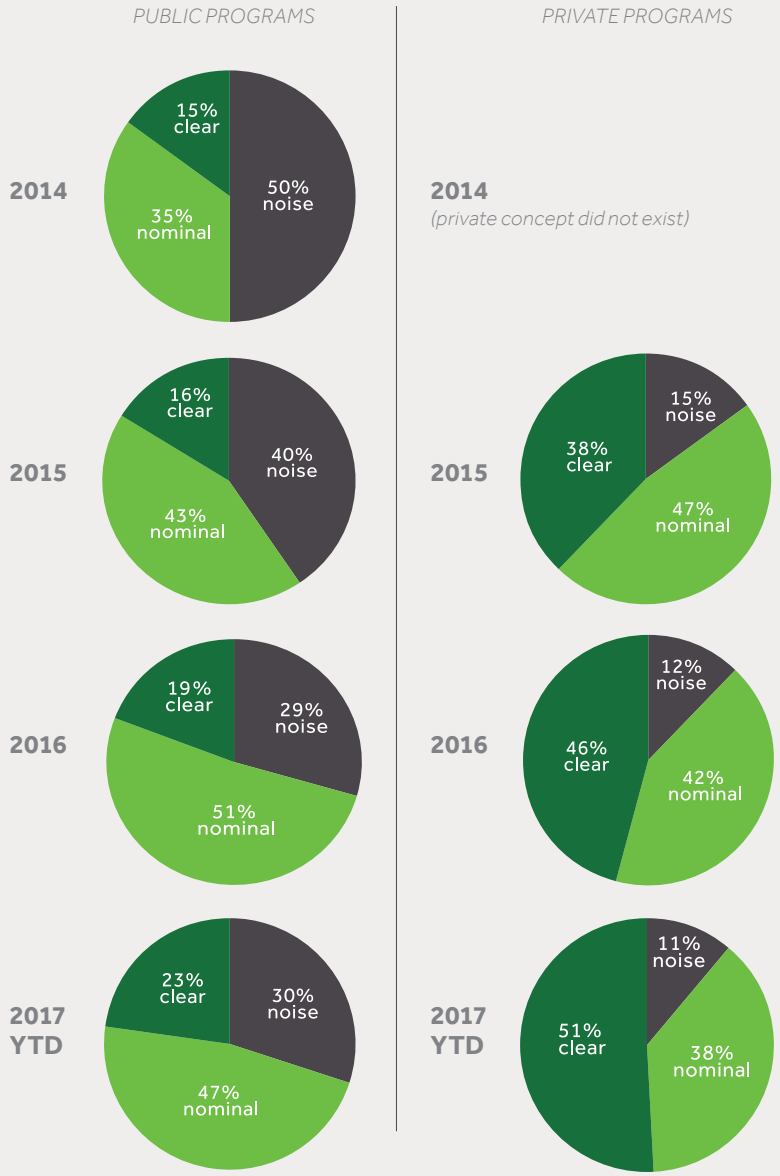


Figure 10: *HackerOne platform signal-to-noise ratio over time.*

HACKERONE

Market Leaders Embrace Vulnerability Disclosure Policies

Today, with thousands of organizations encouraging ethical hacking, 94 percent of the Forbes Global 2000 do not have known vulnerability disclosure policies despite guidance from the United States Department of Defense, Food and Drug Administration, National Highway Traffic Safety Administration, National Telecommunications and Information Administration, National Institute of Standards and Technology, and Federal Trade Commission — to name a few. Nearly 200 organizations rely on the HackerOne platform for their VDP, including the The U.S. Department of Defense, LinkedIn, NewRelic and General Motors.

Given the increased concern about IoT and connected device security, Panasonic is the only consumer electronics company with a public VDP on the Forbes Global 2000 list. Major industry conglomerates, including General Electric, Siemens, Honeywell International, ABB, and Philips, have public policies. Over 50 percent of the Forbes top software/programming companies have a VDP and in many cases offer hackers incentives with bug bounty programs, including Microsoft, Snapchat, Adobe, Symantec, Salesforce.com, and Intuit.

Starbucks is the only restaurant on the list with a VDP. Another major restaurant company, McDonald's, made the news in January 2017 due to its lack of a clear VDP. In retail, Home Depot also does not have a policy, even after agreeing to a $25 million settlement for its 2014 security breach that impacted 50 million customers.

Vulnerability Disclosure Policy Statistics

Based on the 2017 Forbes Global 2000 list of the largest publicly traded companies in the world, our research team searched the Internet looking for ways a friendly hacker could contact a company to disclose a vulnerability.

94%

of the **Forbes Global 2000** do not have known vulnerability disclosure policies.

14%

Five of 36 conglomerates have vulnerability disclosure programs, including **General Electric**, **Siemens**, **Honeywell International**, **ABB**, and **Philips**.

8%

Two out of 24 airlines, **United Airlines** and **Lufthansa**, have vulnerability disclosure policies.

10%

Three out of 31 auto and truck manufacturers have policies. They are **General Motors**, **Tesla** and **Fiat Chrysler Automobiles**.

1

Starbucks is the only restaurant on the list with a vulnerability disclosure or bug bounty program.

54%

of the top software/programming companies, 54% have programs: **Microsoft**, **Oracle**, **SAP**, **VMware**, **Adobe Systems**, **Symantec**, **Salesforce.com**, and **Intuit** (13 of 24).

15%

Three out of 20 consumer financial services, including **Visa**, **MasterCard** and **PayPal** have programs.

9%

Six out 64 Major Banks have vulnerability disclosure policies: only **JPMorgan Chase**, **Citigroup**, **ING Group**, **Danske Bank**, **Swedbank**, and **Royal Bank of Scotland**.

Federal Agencies Recommend VDPs

A vulnerability disclosure policy (VDP) is an organization's formalized method for receiving vulnerability submissions from the outside world. It instructs hackers on how to file vulnerability reports, and defines the organization's internal process for handling those reports. Federal agencies and standards bodies recommend VDPs for all organizations that take security seriously. The practice has been defined in ISO 29147. A VDP is the "if you see something, say something" for software vulnerabilities. Before launching a bug bounty program, organizations are advised to establish a VDP.

NHTSA
www.nhtsa.gov

"Automotive industry members should consider creating their own vulnerability reporting/ disclosure policies, or adopting policies used in other sectors or in technical standards. Such policies would provide any external cybersecurity researcher with guidance on how to disclose vulnerabilities to organizations that manufacture and design vehicle systems."

- National Highway Traffic Safety Administration (NHTSA), "Cybersecurity Best Practices for Modern Vehicles"

FDA

"(Medical device) Manufacturers should adopt a coordinated vulnerability disclosure policy."

- Food and Drug Administration (FDA), "Management of Cybersecurity in Medical Devices"

"The lesson for other businesses? Have an effective process in place to receive and address security vulnerability reports. Consider a clearly publicized and effective channel (for example, a dedicated email address like security(@) yourcompany.com) for receiving reports and flagging them for your security staff."

-Federal Trade Commission (FTC), "Start with Security"

Companies' Perception of Hacker-Powered Programs

HackerOne asked 600 of its customers about their perceptions of hackers' value to security.

95% said they'd recommend hacker-powered security to their peers at other companies. It's efficient, it's cost-effective, and it gets results, they stated.

78% work with hackers to better protect their customers while **72%** say they work with hackers to protect their technology and brand, and **57%** work with hackers because it's a security best practice.

59% started a bug bounty program to give a boost to internal teams, **58%** run bug bounty programs to figure out where their tech is most vulnerable, and **47%** wanted to create a structure for working with hackers.

1 OUT OF EVERY 3 RESPONDENTS SAID THEY'RE NOW BETTER EQUIPPED TO IMPROVE THE SECURITY DEVELOPMENT LIFECYCLE.

Other beneficial business impacts cited: doing less traditional penetration testing, and spending less money to find vulnerabilities.

#1 Security Concern: Exploited Vulnerabilities

The most common worry is security vulnerabilities being exploited (73%), followed by customer data and intellectual property theft (52%), and inherited security debt (42%). When asked about personal security worries relating to connected devices, respondents named identity theft (68%), access to credit cards or bank details (64%), and access to personal details (63%).

Time-Bound Security Testing

Companies and governments are increasingly turning to hacker-powered security to supplement traditional penetration testing. By setting up private, time-bound testing programs like the HackerOne Challenge, customers can capture the value of the hacker-powered model in new situations, such as testing web and mobile applications before deployment. Learn More

Who are Hackers and Why Do They Hack?

While most believe hackers hack for the payday, money isn't the only motivation. HackerOne's 2016 Bug Bounty Hacker Report found that motivations like enjoyment (70%), personal challenge (66%) and doing good in the world (51%) are about as common as the desire to make money (72%).

Regardless of their motivations, the good news for hackers is that many of them can make a living doing what they love. Seventeen percent said they rely solely on bug bounty programs for their income, while 26 percent said that between 76 percent and 100 percent of their incomes comes from bug bounty programs.

As more bug bounty programs are created, more hackers of all stripes are signing up. Over 100,000 hackers are registered on HackerOne, and they've earned more than $17 million in bounties. Hackers hail from 90 countries, with the biggest groups coming from India and the United States.

Hacker: one who enjoys the intellectual challenge of creatively overcoming limitations, also known as white hat, ethical hacker, or security researcher.

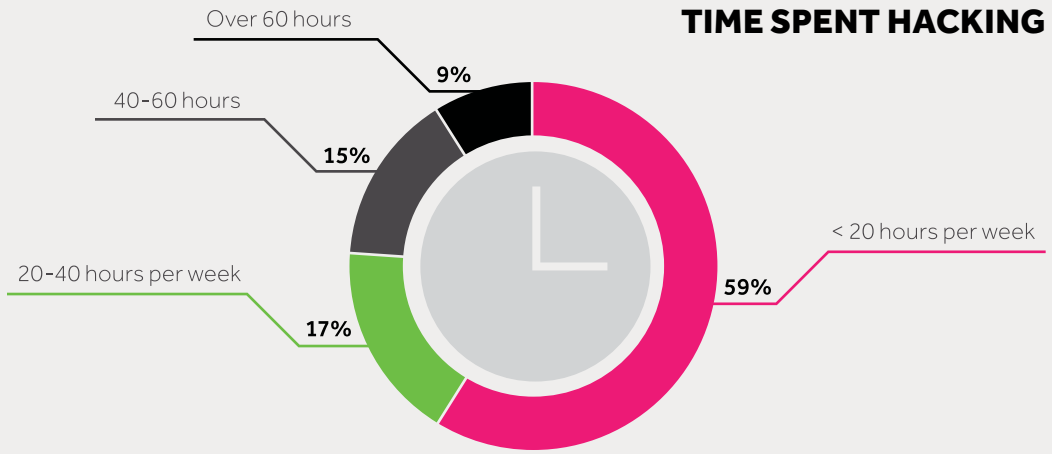


Figure 11: *Proportion of hackers by average amount of weekly time they spend hacking.*

WHY DO HACKERS HACK?

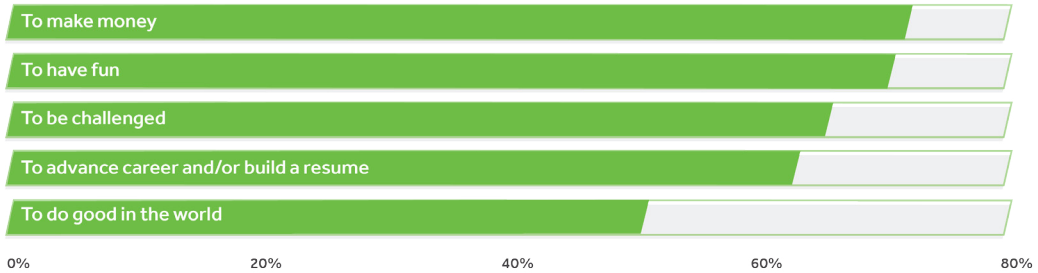


Figure 12: *What motivates hackers. HackerOne surveyed 600 hackers to better understand what motivates them to hack.*

AGE OF A HACKER

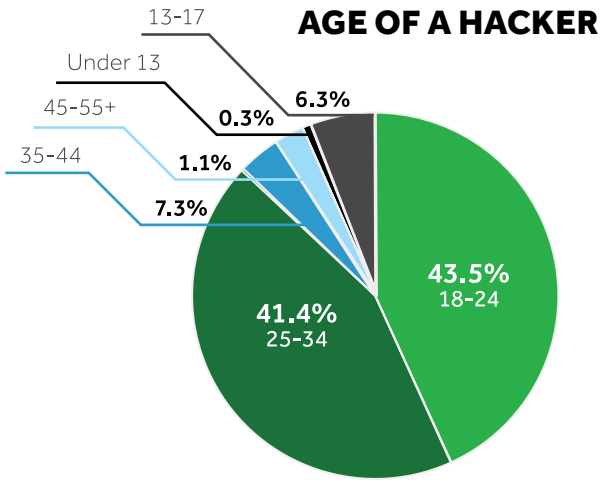
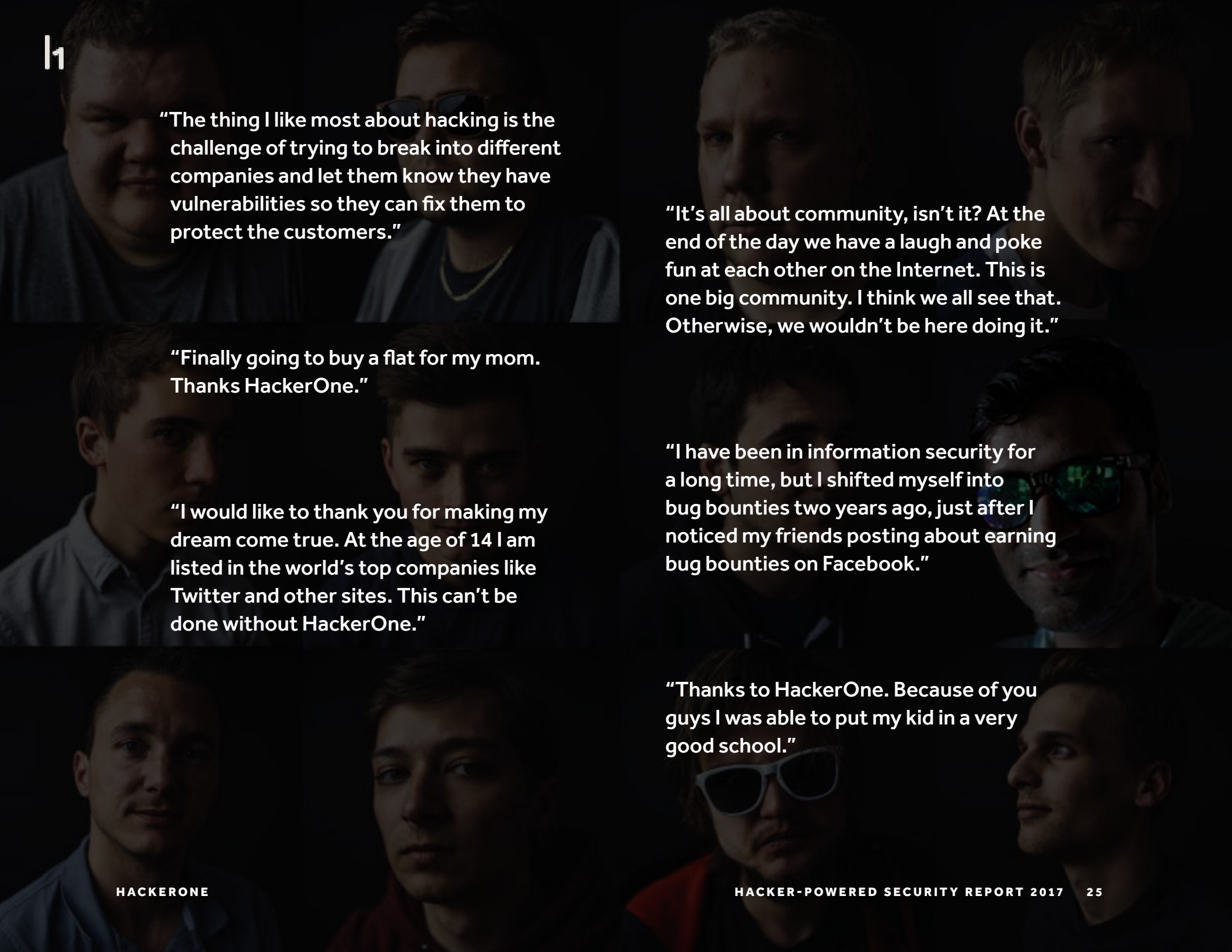


Figure 13: *Over 90% of hackers are under 34 years old. For more on the hacker community, what motivates hackers and how they hack check out the full report: 2016 Bug Bounty Hacker Report*

5 MOTIVATIONS OF SECURITY RESEARCHERS

While hackers have diverse motivations, I Am The Cavalry provides a framework to encourage discussion and appreciation why hackers investigate security flaws: Protect, Puzzle, Prestige, Profit, and Politic.
Read more



"The thing I like most about hacking is the challenge of trying to break into different companies and let them know they have vulnerabilities so they can fix them to protect the customers."

"Finally going to buy a flat for my mom. Thanks HackerOne."

"I would like to thank you for making my dream come true. At the age of 14 I am listed in the world's top companies like Twitter and other sites. This can't be done without HackerOne."

"It's all about community, isn't it? At the end of the day we have a laugh and poke fun at each other on the Internet. This is one big community. I think we all see that. Otherwise, we wouldn't be here doing it."

"I have been in information security for a long time, but I shifted myself into bug bounties two years ago, just after I noticed my friends posting about earning bug bounties on Facebook."

"Thanks to HackerOne. Because of you guys I was able to put my kid in a very good school."

Comparing Customer and Hacker Surveys

From the perspective of customers that establish bug bounty programs, what do they believe motivates hackers? How does this line up with what the hackers actually say motivates them?

Customers Think...	What Hackers Actually Say...
77% think hackers hack for financial gain	72% hack to make money
40% believe they do it for the challenge	51% hack to do good in the world

57 percent of hackers say they even took part in bug bounty programs that didn't offer bounty payouts. For more on why hackers hack, check out the 2016 Bug Bounty Hacker Report.

Safer Products, Thanks to Hackers

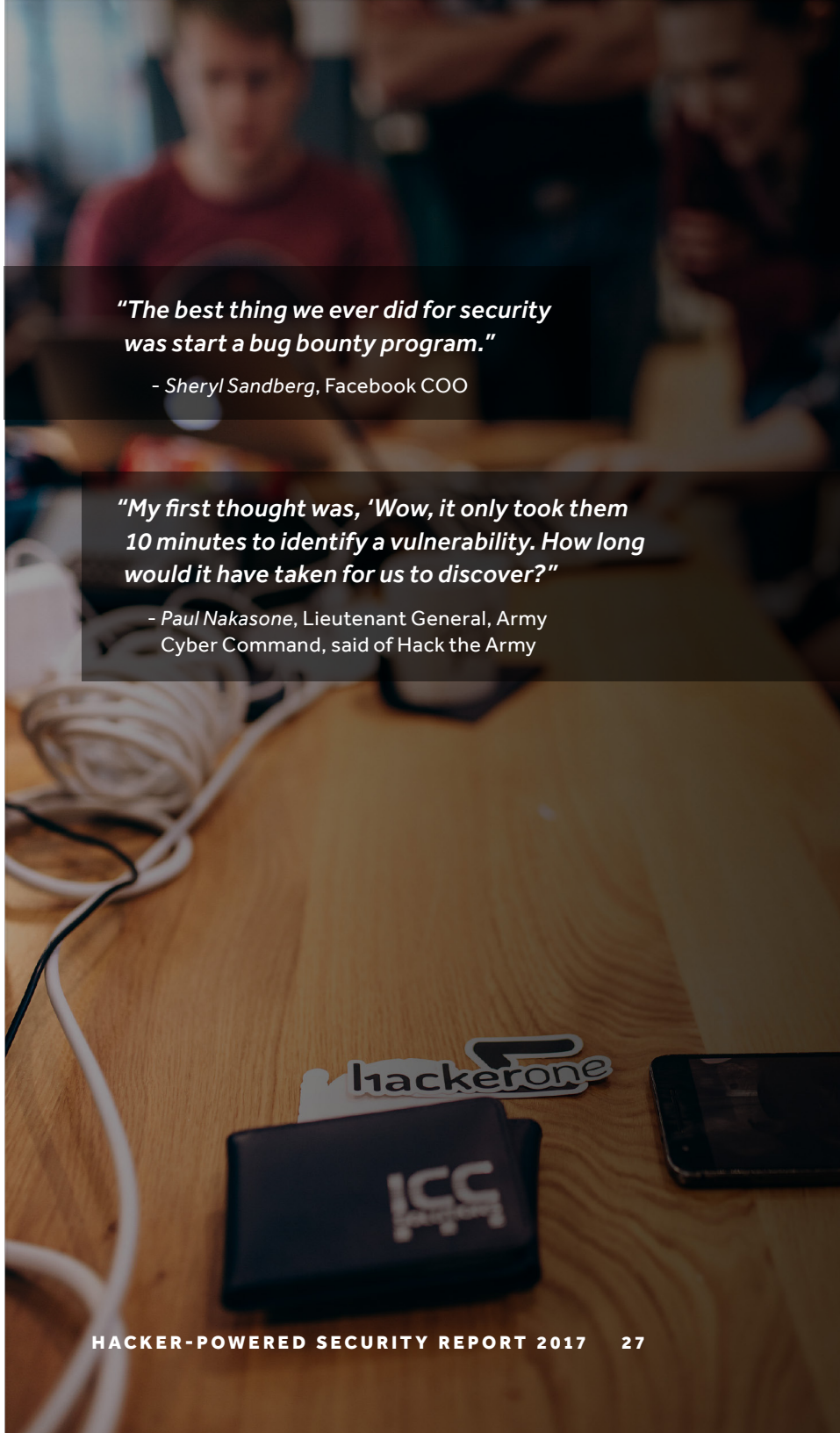
Over 30 years after the first "bug" bounty program, relying on hackers is a best practice, not a stealth operation. In 2016, the number of hackers on the HackerOne platform grew nearly 300 percent, bounty payments are on the rise, and organizations that rely on hackers are singing their praises. Companies in all verticals have discovered that hackers can find vulnerabilities faster and more cost effectively than internal development teams. The rise of hacker-powered security translates to greater confidence in product security. Here's how HackerOne sees the future of bug bounty programs:

More industries outside technology will widely adopt hacker-powered security. With market leaders already running successful bug bounty programs, more companies in more industries will look to improve their security.

Organizations will have to compete for the best hacker talent. Bounties are rising, and companies have seen the value of using monetary incentives, and other tools to attract talent to their program.

As online criminals innovate, hackers will close gaps in security. Attackers aren't going anywhere — in fact, they're getting smarter. Organizations with bug bounty programs will lead the way in identifying and fixing product flaws before they make the news.

For the most comprehensive guide on how plan, launch, and operate a successful bug bounty program, check out The Bug Bounty Field Manual.



"The best thing we ever did for security was start a bug bounty program."

- Sheryl Sandberg, Facebook COO

"My first thought was, 'Wow, it only took them 10 minutes to identify a vulnerability. How long would it have taken for us to discover?"

- Paul Nakasone, Lieutenant General, Army Cyber Command, said of Hack the Army

Methodology and Sources

Findings in this report were collected from the HackerOne platform using HackerOne's proprietary data based on over 800 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.

2017 HackerOne Customer Survey: In May 2017, HackerOne surveyed 600 customers from the U.S. and EMEA who used the platform in the most recent 30 day period. Respondents came from a variety of industries, including Software/IT/Hardware industries (53%), followed by finance and banking, retail, hospitality and education, and others. Fifty-seven percent described the organization or team they reported to as engineering, followed by security (24%), IT (10%), and other. The majority of those surveyed described their titles in descending order as managers, followed by individual contributors, director level, C-level executives and vice president.

2016 Bug Bounty Hacker Report: The report was based on over 600 responses to the 2016 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 bug bounty and vulnerability disclosure platform with the largest community of ethical hackers and the most hacker-powered security programs.

Since our first customer joined in 2013, over 800 programs have launched on HackerOne, collectively paying out more than $17 million in cash bounties to hackers and security researchers. Nearly 50,000 security vulnerabilities have been fixed and rendered unexploitable by malicious actors. The connected world is becoming more secure.

Contact HackerOne