HACK FOR GOOD // EUGENE

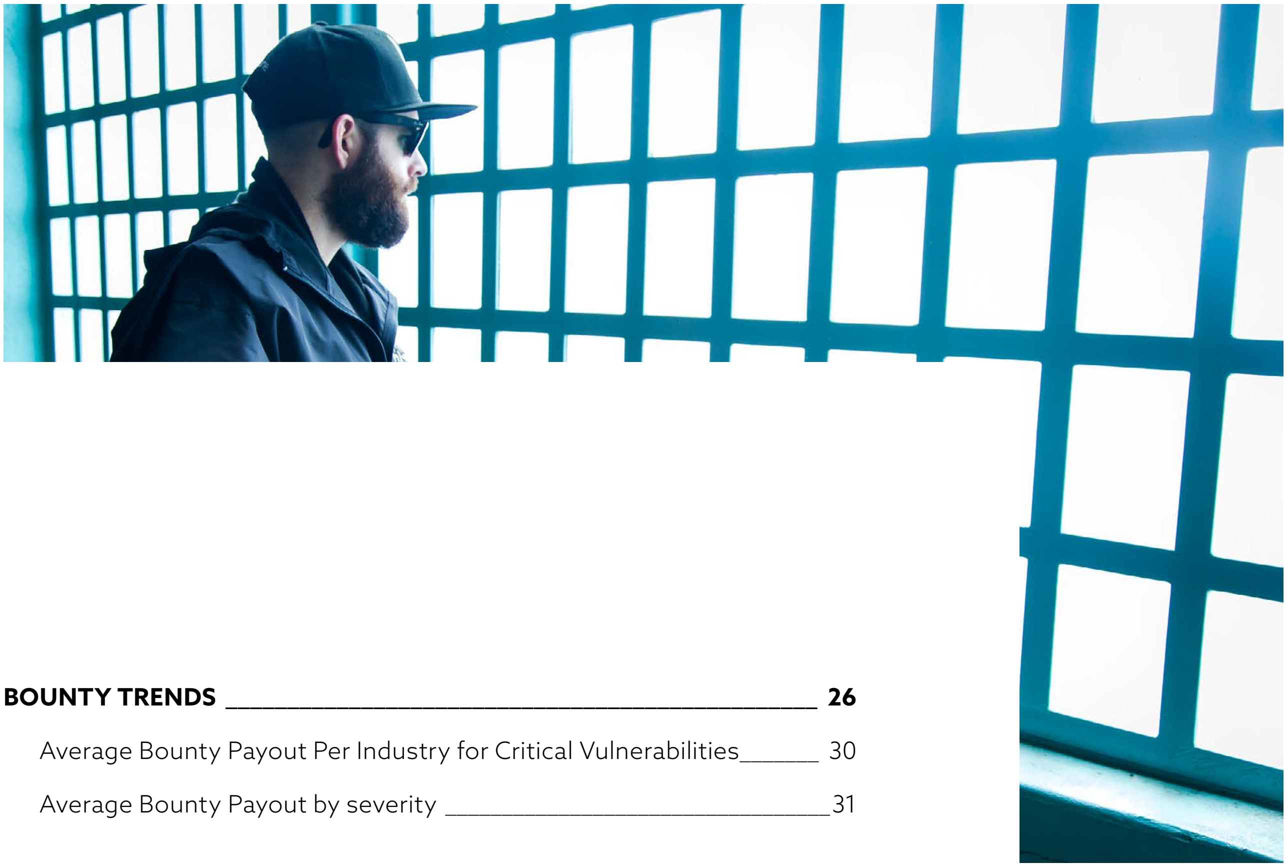
THE 4TH ANNUAL

# HACKER POWERED SECURITY REPORT

ECOMMERCE

hackerone

# CONTENTS



/// OVERVIEW

# IMPORTANT CONCEPTS

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

**HACKER-POWERED SECURITY:** Any security-enhancing activity resulting from voluntary work performed by external experts, i.e. hackers. Common examples include private bug bounty programs, public bug bounty programs, time-bound bug bounty programs, hacker-powered penetration testing for compliance, and vulnerability disclosure policies. With hacker-powered security testing, organizations can identify high-value bugs faster with help from the results-driven ethical hacker community.

**VULNERABILITY:** A weakness in software, business logic, hardware, internal rules, or online services that can be exploited.

**HACKTIVITY:** Hacker activity published on the HackerOne platform.

**VULNERABILITY DISCLOSURE POLICY (VDP):** An organization's formalized method for receiving vulnerability submissions from the outside world, sometimes referred to as "Responsible Disclosure." This often takes the form of a "security@" email address. The practice is outlined in the NIST Cybersecurity Framework and defined in ISO standard 29147.

**BUG BOUNTY PROGRAM:** Encourages hackers, through the use of incentives, to identify and report potential security vulnerabilities before they can be exploited. A public program allows any hacker to participate for a chance at a bounty reward. A private program limits access to select hackers who are invited to participate. Focused programs can also be time-bound, or run as virtual or in-person live events.

**HACKER-POWERED PENTEST:** A bespoke program where select hackers apply a structured testing methodology and are rewarded for completing security checks, and security teams receive instant results and compliance-ready reports.

Total registered hackers

**830K+**

Total valid vulnerabilities submitted

**181K+**

Total bounties paid

**$107M+**

Reports resolved in 2019

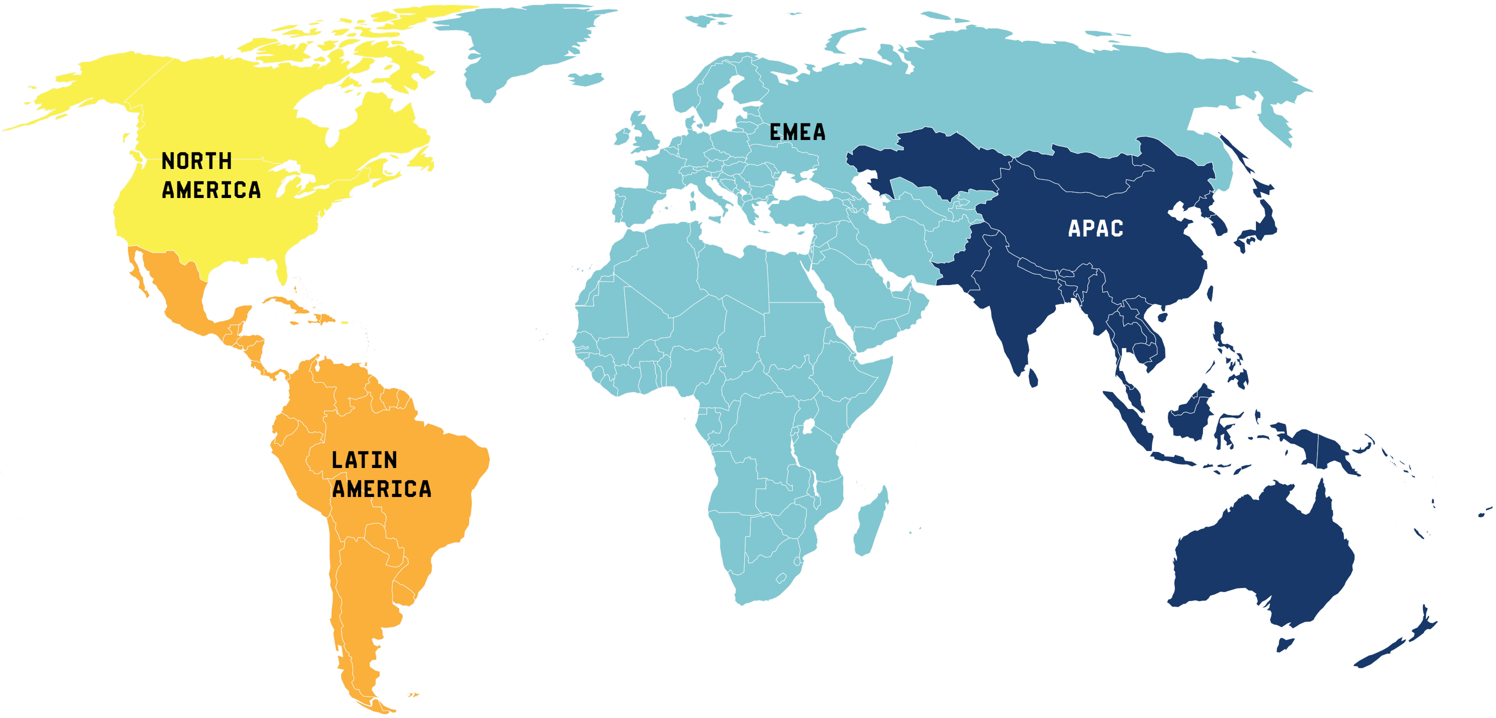
**37,259**

Bounties paid over the past 12 months

**$44,754,742**

$ per resolved report

**$979**



# INTRODUCTION

## EVERY ONE HUNDRED AND EIGHTY SECONDS, A HACKER REPORTS A VULNERABILITY.

This is a time of unprecedented challenges. We face never-before-seen threats in the digital and physical worlds. If this past year has taught us anything, it is this: we need to leave behind our old tools, mindsets, and methods to create a path ahead.

But what does that path look like? COVID-19 has lead organizations across the globe to make unexpected changes to their operations. Businesses are figuring out how to contend with accelerated digital transformation and a surge in digital transaction volume. Many have had to expedite their decision to move to the cloud. Companies are hurrying to support hundreds or thousands of employees who are suddenly working remotely. To adapt to changing spending patterns, retail and ecommerce companies have launched new digital products and revenue streams, fighting to keep revenue flowing during a global recession.

In doing so, organizations are opening up new attack surfaces they are unprepared to protect. Protection efforts are left in the hands of security teams who are not staffed to cope. The result? Losses that can be measured in data, revenue, reputational damage, operational disruption, and churn.

There's no such thing as business-as-usual anymore—which means that business-as-usual security can no longer suffice. Security leaders are starting to ask some tough questions. If you're facing resource constraints, how do you design software that's secure from the start? How can you protect software applications as they move to the cloud? How do you scale security on a constantly-evolving attack surface? Is there a way to maintain brand trust and mitigate risk of a breach with such a sharp increase in digital transactions? And with everything else on fire, what about the nuts-and-bolts of compliance and regulations?  The 2020 Hacker-Powered Security Report: Retail & Ecommerce offers an incisive look at the global security landscape for financial services organizations and the hackers who are pushing the envelope to help them.

Around the world, the hacker community grew in size and sophistication, using hacking to build valuable skills, advance their career, earn extra money, and challenge their curiosity. In a hundred countries, hackers had year-over-year earnings growth, and hackers earned bounties for the very first time in a dozen more countries.

Retail and e-commerce businesses are augmenting security frameworks with hackers' human creativity and always-on security efforts. Against a backdrop of unparalleled obstacles, hacker-powered security continued to scale. During global lockdowns, hackers reported 28% more vulnerabilities per month than immediately before the pandemic took hold. For many researchers, hacking became a reliable source of supplemental income during the pandemic.

In this report, we'll explore these trends and their ramifications for businesses worldwide. The future of security starts here.

Global average total cost of a data breach in 2020

**$3.86M**

Average cost of a valid vulnerability

**$979**

# KEY FINDINGS

## 1

*The number of retail ad e-commerce companies adopting hacker powered security has more than doubled in the past year.*

## 2

*In 77% of cases, public bug bounty programs receive their first vulnerability report within the first 24 hours.*

## 3

*Retail & e-commerce firms are among the top 3 fastest industries respond to hackers with a median time to response of 0.6 days.*

hackerone

# HOW COVID-19 IS IMPACTING SECURITY

COVID-19 has thrown the entire world into chaos. We will feel the digital and physical ramifications of the pandemic for decades.

Criminals thrive on chaos. Organizations worldwide were forced to go digital with their product offerings and services. Businesses scrambled to find new revenue streams, creating digital offerings for customers whose lifestyles had dramatically changed. Tens of millions of workers had to work remotely. With this accelerated pace of digital transformation, CISOs had to quickly facilitate new needs—while ensuring the security of existing systems and newly-acquired collaboration tools. Security teams were pushed to the limit. They struggled to maintain existing security measures while working to close newly-opened gaps.

To better understand how COVID-19 has impacted security, HackerOne surveyed security leaders about their challenges during the pandemic. We found that 64% of global security leaders believe their organization is more likely to experience a data breach due to COVID-19, and 30% have seen more attacks as a result of COVID-19. Unfortunately, 30% have seen their security teams reduced due to the pandemic, and a quarter have seen their budgets reduced. The overall chaos and uncertainty has stressed even the most robust security teams.

## THIS IS AN ENTIRELY DIFFERENT BALLGAME.

*"It suddenly thrust us into what some people would say is just a healthcare issue, but it's not. It's an everything issue, isn't it. It's really just changing the way that the world operates and even how hackers operate as well, and I think that's what we're starting to see more and more of."*

**TERESA WALSH**
Global Head of Intelligence, Financial Services ISAC, During ISAC webinar 2020

To adapt to changing attack surfaces, many are turning to hacker-powered security. And hackers are stepping up.

Even during the global recession, hacking has remained a consistent and stable source of income. This past year, new hackers have joined the community at an accelerated rate. Compared with January and February of 2020, as the pandemic took hold, the average number of new hacker signups on the HackerOne platform increased by 56% across April, May, and June. Year over year, April, May, and June of 2020 saw 69% more new hacker signups than the same period in 2019.

Hackers are also more prolific than ever with the monthly average number of incoming bug reports in April, May, and June of 2020 increasing by 28% over January and February, and increasing 24% over the previous year.

Organizations have responded to this much-needed help by awarding 29% more bounties per month, on average, during the April-June period than during January and February.

To learn more, see how HackerOne can help address quickly changing security needs.

# SECURITY LEADERS SEEING OUTBREAK OF CYBERCRIME DURING PANDEMIC

**64%**

Security breach more likely

**30%**

Seeing more attacks

**30%**

Reduced security teams

**25%**

Dealing with budget cuts

In early 2020, as the global pandemic took hold, the Internet Complaint Center at the U.S. Federal Bureau of Investigation reported seeing three- to four-times their typical number of reports. The spike in cybercrime also prompted the U.S. National Counterintelligence and Security Center to issue a warning about "threat actors" increasing their attacks on medical research organizations. A related study revealed that large-scale breaches increased 273% in early 2020, compared with 2019.

In the summer of 2020, HackerOne surveyed 1,400 global security leaders at large companies across North America, Europe, and Asia-Pacific, to learn more about their challenges during the pandemic. Unfortunately, what many are dealing with in reality reflects the warnings offered earlier in the year. The impact of both challenges are forcing security teams to face more threats while dealing with diminished resources.

Nearly two-thirds (64%) of global security leaders believe their organization is more likely to experience a data breach due to COVID-19, and 30% have seen more attacks since the start of the pandemic. Unfortunately, 30% have seen their security teams reduced and one-quarter have seen their budgets reduced since the pandemic began.

But as the pandemic has increased threats and decreased resources, it has also increased distractions. More than a third (36%) of security leaders say that digital transformation initiatives have accelerated as a result of COVID-19, and 30% have had to switch priorities from application security to securing new work-from-home and collaboration tools.

Many are now looking to hacker-powered security to augment their own resources and offer a pay-for-results approach that's more justifiable under tightened budgets. As a result of the challenges posed by COVID-19, 30% of security leaders say they are more open to accepting vulnerability reports from third party researchers about information security issues.

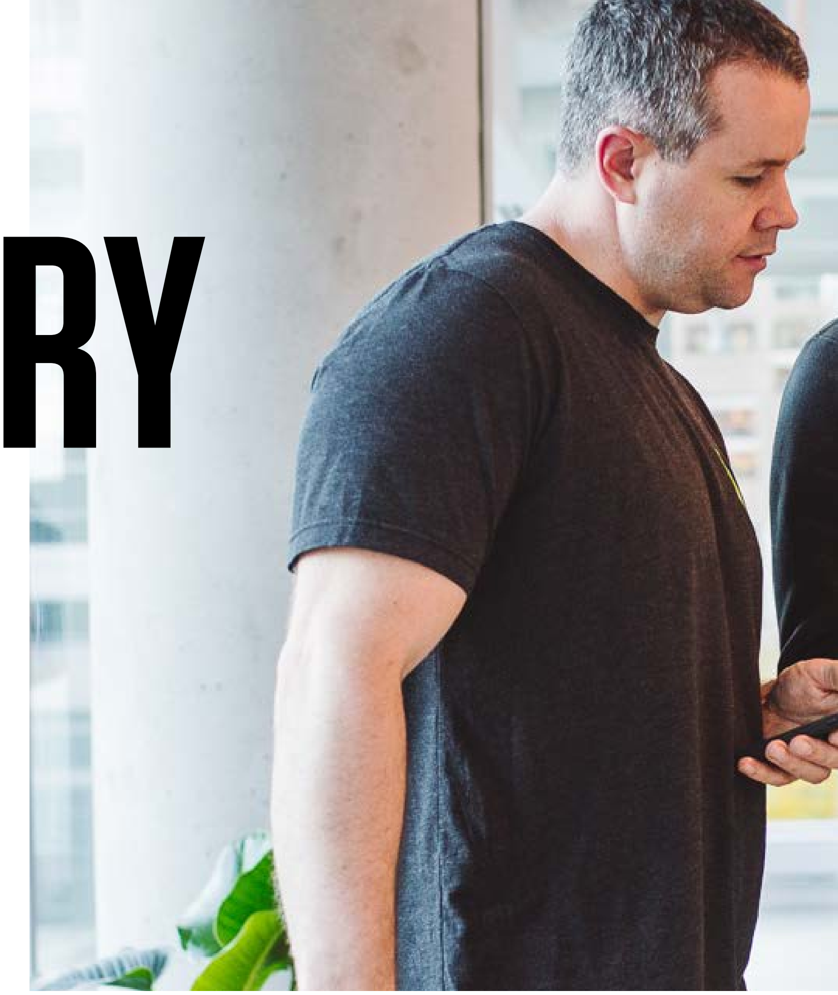
Learn how HackerOne can help you quickly add resources to your security efforts.

| GLOBAL HEADLINE | UK | FRANCE | GERMANY | AUSTRALIA | SINGAPORE | USA | CANADA |
|---|---|---|---|---|---|---|---|
| **36%** of security leaders say that digital transformation initiatives have accelerated as a result of COVID-19 | 39% | 32% | 34% | 36% | 37% | 35% | 37% |
| **31%** of security leaders say they have had to go through a digital transformation ahead of the planned roadmap as a result of COVID-19 | 34% | 28% | 29% | 22% | 39% | 32% | 33% |
| **30%** of security leaders have had to switch priorities during the pandemic from application security to securing the use of working from home and collaboration tools | 34% | 26% | 41% | 28% | 29% | 30% | 27% |
| **30%** of security leaders have seen more attacks on their IT systems as a result of COVID-19 | 31% | 36% | 28% | 33% | 21% | 34% | 30% |
| **30%** of security leaders say their security teams have been reduced during the pandemic | 37% | 28% | 28% | 35% | 30% | 24% | 30% |
| **30%** of security leaders say that as a result of the challenges posed by COVID-19, they are more open to accepting reports from third party researchers about information security issues | 30% | 33% | 34% | 32% | 21% | 34% | 26% |
| **A quarter** of security leaders say that information security budgets have been negatively impacted as a result of COVID-19 | 29% | 30% | 23% | 26% | 24% | 27% | 27% |
| **64%** of global security leaders believe their organisation is more likely to experience a data breach due to COVID-19 | 69% | 70% | 70% | 55% | 58% | 57% | 68% |
| **66%** of global security leaders feel under scrutiny to prove the business takes information security seriously | 72% | 62% | 61% | 53% | 76% | 61% | 75% |

**Figure 1:** Cybersecurity trends during COVID-19

CHAPTER 2 //

# INDUSTRY SCORE-CARDS



Hacker-powered security comes in many flavors, from simply providing a clear path for anyone to alert you to a potential risk, to integrating hacker-powered methods directly into your security, testing, and software development processes. Programs can be open to anyone or limited to trusted, vetted hackers; free or pay-for-results; customized or turnkey; run internally or completely managed by experts. They can even be used to assess security measures, retest bug fixes, increase the security awareness of development, and more. With this flexibility, hacker-powered security can meet the security needs of any organization.

## 5X

Public programs have 5x the number of hackers reporting valid vulnerabilities as private programs

## 40%

of programs started in the past year were in Computer Software and Internet & Online Services

## BUG BOUNTY PROGRAMS ARE DOMINATED BY COMPANIES IN COMPUTER SOFTWARE AND INTERNET & ONLINE SERVICES

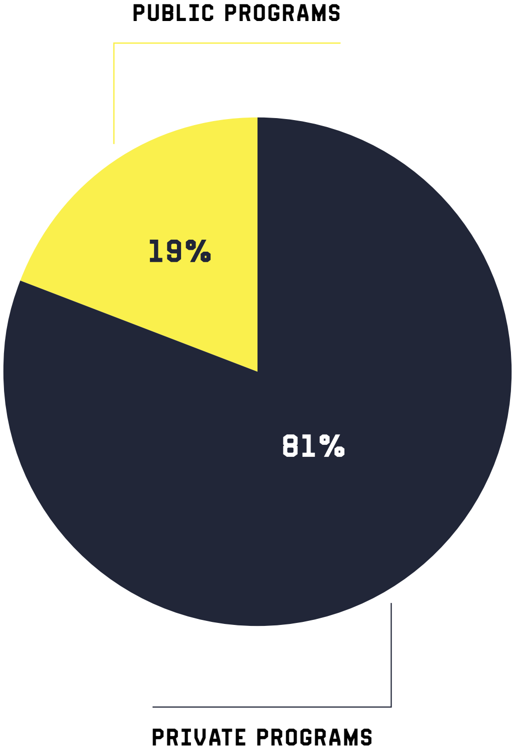


**Figure 2:** Percentage of public vs private programs.

Most organizations begin with a vulnerability disclosure policy (VDP). It offers an easy, open process for anyone who spots a potential vulnerability to report it to an organization's appropriate teams. Pentests put continuous hacker talent and creativity to work for compliance and other requirements. The bug bounty program is the most advanced form of hacker-powered security, and has a wide range of applications and approaches. It gives hackers a monetary incentive— the bounty—to search for and report vulnerabilities. Bounty programs can be public or private, continuous or time-bound.

Public bug bounty programs, like those of Paypal, Deliveroo, Shopify and Starbucks are open to everyone, while private programs require that individual hackers are invited or accepted via an application process to participate. Public programs are open to the widest range of hacker diversity and therefore produce superior results. On average, public programs have nearly five times the number of hackers reporting valid vulnerabilities versus private programs. Similar to past years, private programs make up 81% of all bug bounty programs on HackerOne and public programs make up the remaining 19%.

# HOW EACH INDUSTRY STACKS UP

When you dig into industry-specific data, things get a bit more interesting. While Computer Software and Internet & Online services are most likely to have a bug bounty program, last year HackerOne saw a 50% increase in retail & e-commerce businesses adopting hacker-powered security. But others are quickly adopting hacker-powered security. Industries with year-over-year program growth of 200% or greater include Computer Hardware (250%), Consumer Goods (243%), Education (200%), and Healthcare (200%), while Media & Entertainment grew by 164% and Financial Services and Computer Software each grew by more than 75%.

Across the board, industries are paying more bounties to more hackers, too. Industries paying more than $1 million / €850,000 / ¥7 million in bounties in the past year include Financial Services ($2,286,351), Retail & Ecommerce ($1,004,045), Media & Entertainment ($1,826,974), and Automotive ($1,048,090).

| | BOUNTY PROGRAMS | | | | BOUNTY AWARDS | |
|---|---|---|---|---|---|---|
| | PRIVATE | PUBLIC | SHARE OF TOTAL | SHARE OF NEW | 2019 | % OF TOTAL |
| Computer Hardware & Peripherals | 93% | 7% | 3% | 1% | $415,994 | 0.9% |
| Computer Software | 82% | 18% | 20% | 16% | $16,263,982 | 36.3% |
| Consumer Goods | 98% | 2% | 2% | 4% | $253,763 | 0.6% |
| Cryptocurrency & Blockchain | 57% | 43% | 4% | 2% | $518,565 | 1.2% |
| Electronics & Semiconductor | 76% | 24% | 1% | 0% | $381,250 | 0.9% |
| Financial Services & Insurance | 87% | 13% | 8% | 9% | $2,286,351 | 5.1% |
| Government International | 65% | 35% | 1% | 1% | $134,729 | 0.3% |
| Government NA Federal | 90% | 10% | 1% | 2% | $667,228 | 1.5% |
| Government NA Local | 100% | 0% | 0% | 0% | $19,583 | 0.0% |
| Healthcare | 100% | 0% | 1% | 1% | $104,050 | 0.2% |
| Internet & Online Services | 79% | 21% | 27% | 24% | $16,079,195 | 35.9% |
| Media & Entertainment | 80% | 20% | 7% | 7% | $1,826,974 | 4.1% |
| OTHER | 74% | 26% | 11% | 19% | $1,525,877 | 0.5% |
| Professional Services | 84% | 16% | 3% | 3% | $256,229 | 0.6% |
| Retail & eCommerce | 87% | 13% | 4% | 3% | $1,004,045 | 2.2% |
| Telecommunications | 88% | 12% | 1% | 1% | $2,497,042 | 5.6% |
| Travel & Hospitality | 93% | 8% | 2% | 1% | $519,885 | 1.2% |
| **Overall** | **81%** | **19%** | | | **$44,754,742** | |

BREAKDOWN

## THE BIGGEST BRANDS STILL LAG:

# FORBES GLOBAL 2000

Each year, HackerOne analyzes the Forbes Global 2000 list of the world's most valuable public companies as one benchmark for public VDP adoption. Based on the 2020 Forbes Global list, 82% of the Forbes Global 2000 do not have a known policy for vulnerability disclosure as of July 2020. That's a huge improvement compared to 93% on the 2017 list and 94% of the 2016 list, but shows that less than 1 in 5 of the world's most valuable public companies are utilizing this important security mechanism.

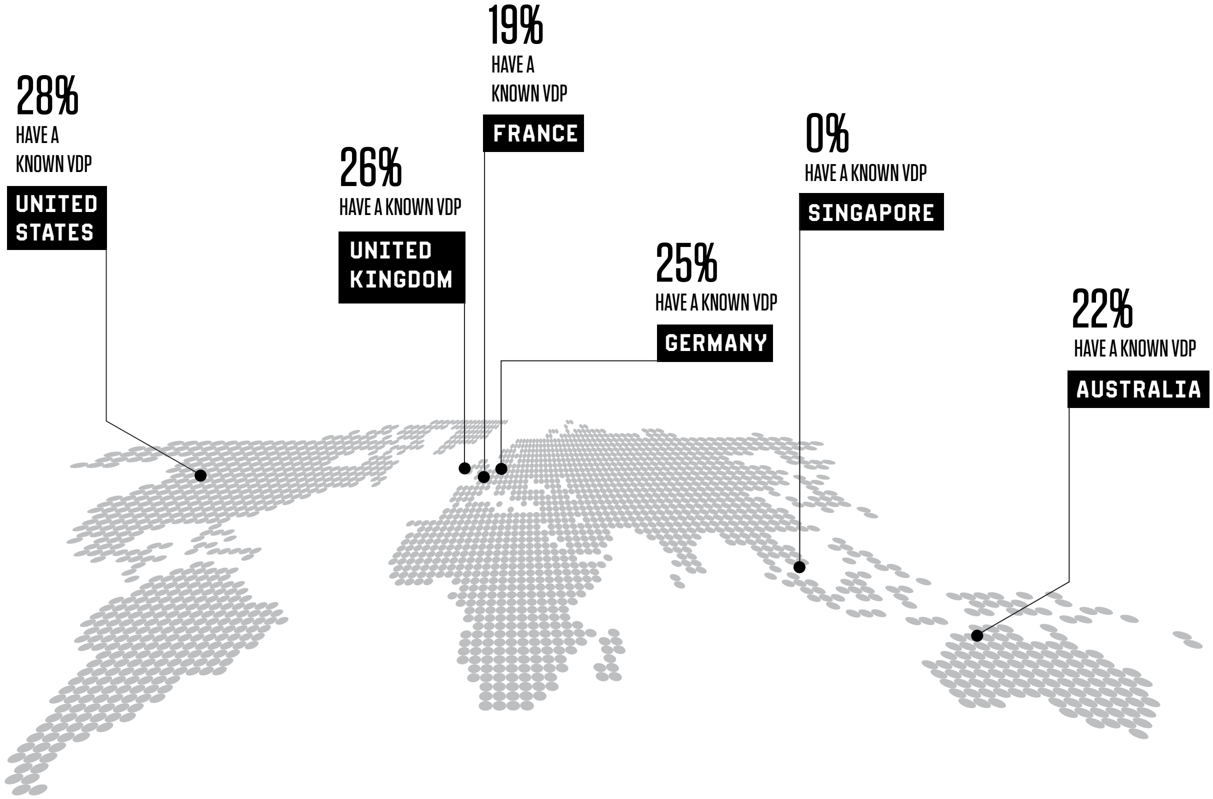


**Figure 4:** Share of Forbes Global 2000 companies in various countries that have a known VDP.

**63%**

Of global organizations require IT suppliers to have a VDP

**82%**

Of Fortune Global 2000 companies do not have VDPs

VDP adoption varies widely across industries and regions. Only 13% of Global 2000 Transportation companies have VDPs, including Toyota, General Motors, Lufthansa, Tesla, American Airlines. Just 21% of Healthcare companies have a known VDP. Approximately one-third of those in Telecommunications & Media (35%) and Financial Services (32%) have known VDPs, including AT&T, Citigroup, JPMorgan Chase, and ING. Computer Software leads in the deployment of VDPs with 69% adoption.

The pace of adoption is extremely slow and organizations continue to push for more progress.  In North America, the U.S. Department of Justice offers a framework and the U.S. Department of Homeland Security provides a template and issued a Binding Operational Directive requiring agencies to establish a VDP. In EMEA, the European Union Agency for Cybersecurity (ENISA) has a "good practices guide" and the National Cyber Security Centre in Netherlands publishes guidelines. In APAC, the Singapore Infocomm Media Development Authority acts as a central point of disclosure for the country's telecommunications industry, and the "Standards for Handling Software Vulnerability Information and Others" has been offered by the Japan Ministry of Economy, Trade and Industry since 2004.

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

# CREATING A VULNERABILITY DISCLOSURE POLICY

Relying only on your internal security team to keep your company safe isn't just unreasonable, it's impossible. Your team doesn't have enough hours in the year to possibly search for, detect, and investigate every possible security risk across your business. Sometimes, they don't have the skill sets or expertise. So, enlisting everyone's help in plugging security gaps isn't just good for security, it's good for your brand, your reputation, and your customers' trust.  It's also a best practice and a regulatory expectation.

A Vulnerability Disclosure Policy (VDP) is the first step in helping protect your company from an attack or premature vulnerability release to the public. It gives hackers and security researchers clear guidelines for reporting security vulnerabilities to the proper person or team within your company.

VDPs are often referred to as the "see something, say something" of the internet. When a skillful eye spots a potential risk, you want to make it as easy and straightforward as possible for them to make you aware. Without it, those vulnerabilities remain unknown, unfixed, and potentially unleashed to people outside your organization, exposing your business and your brand to unnecessary risk or disastrous consequences.

But the VDP paradox is that, even though 63% of global organizations say they require their IT suppliers to have a VDP, more than 82% of the Fortune Global 2000 companies do not have VDPs of their own! Security is a business imperative, and actively encouraging hackers to alert you to vulnerabilities is good business.

## 5 CRITICAL COMPONENTS FOR EVERY VDP PROGRAM

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

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

**"Safe Harbor"**
Assures that reporters of good faith will not be unduly penalized.

**Process**
The process finders use to report vulnerabilities.

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

HackerOne has revolutionized VDPs to make it easy to work directly with trusted hackers to resolve critical security vulnerabilities. Our VDP structure is based on the recommended practice outlined in the Cybersecurity Framework by the United States' National Institute of Standards and Technology (NIST). Since 2012, HackerOne has partnered with thousands of organizations to unlock the security value of the global hacking community. Now, HackerOne has become the only hacker-powered security vendor to receive FedRAMP authorization.

# INDUSTRY ADOPTION

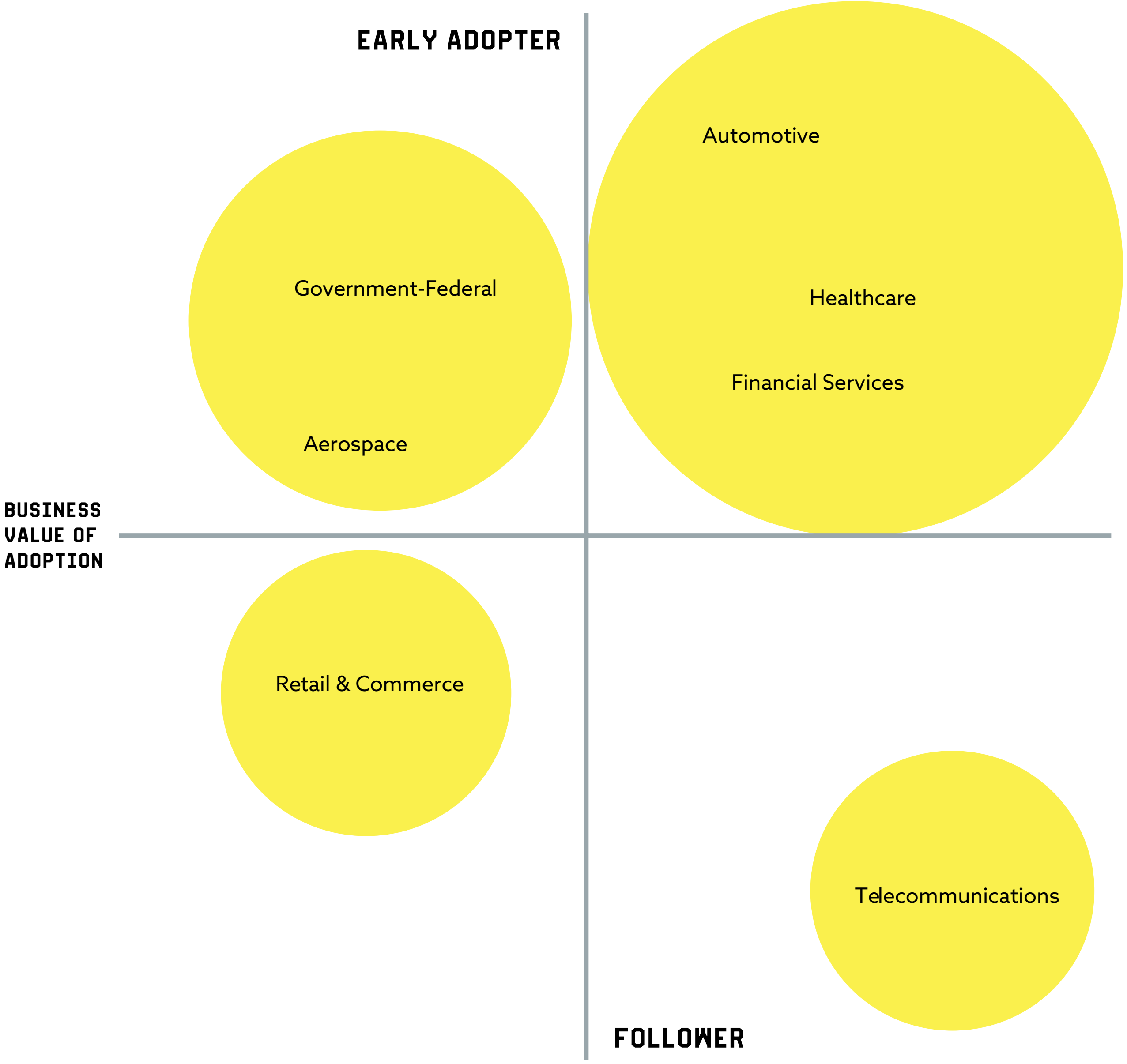


**Figure 5:** Industry adoption

# THE PACE OF RESOLUTION VARIES BY INDUSTRY

In 77% of cases, public bug bounty programs receive their first vulnerability report within 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-vulnerability resolution for all programs. A speedy resolution significantly reduces the risk of a breach. Speed is also important to hackers, who prefer a fast first response to their vulnerability report submissions. This lets hackers know that their report was received and is being investigated. Once a report is validated, hackers prefer to be awarded their earned bounty as quickly as possible.

Nearly all industries respond to hackers in less than one day, with the fastest being Automotive and Media & Entertainment companies. Both sectors have median first response times of less than 4 business hours. Time to resolution and time to bounty award vary widely across the industries: Cryptocurrency & Blockchain (11.7 days) and Professional Services (16.0 days) are among the fastest, while Telecommunications (40.3) and Government Federal NA (39.0) are the slowest.

For time to bounty, the fastest industries are Financial Services & Insurance (0.9), and Retail & eCommerce (1.6). Government Federal NA is, by far, the slowest to pay bounties, with a median time to bounty of 27.1 days. The next slowest is Telecommunications, which pays nearly twice as fast, with a median time to bounty of 13.6 days.

## TIME TO RESPONSE, RESOLUTION, BOUNTY
(DAYS, MEDIAN)

| | TIME TO FIRST RESPONSE (HOURS) | TIME TO RESOLUTION (DAYS) | TIME TO BOUNTY (DAYS) |
|---|---|---|---|
| Computer Hardware & Peripherals | 0.9 | 30.6 | 9.2 |
| Computer Software | 0.8 | 22 | 4.8 |
| Consumer Goods | 0.7 | 20.1 | 2 |
| Cryptocurrency & Blockchain | 0.8 | 11.7 | 3.1 |
| Electronics & Semiconductor | 0.4 | 17.2 | 4.3 |
| Financial Services & Insurance | 0.8 | 16.2 | 0.9 |
| Government International | 0.6 | 20.8 | 3.0 |
| Government NA Federal | 0.6 | 39 | 27.1 |
| Government NA Local | 1.5 | 7.6 | 0.2 |
| Healthcare | 0.9 | 24.8 | 2.3 |
| Internet & Online Services | 0.7 | 18.9 | 5.7 |
| Media & Entertainment | 0.4 | 25.1 | 6 |
| OTHER | 1.7 | 17.9 | 6.2 |
| Professional Services | 1.2 | 16 | 1.7 |
| Retail & eCommerce | 0.6 | 20.4 | 1.6 |
| Telecommunications | 0.9 | 40.3 | 13.6 |
| Travel & Hospitality | 0.6 | 19.6 | 1.6 |
| **Overall** | **5.4** | **21.8** | **4.8** |
| APAC | 0.53 | 18.3 | 3.7 |
| North America | 0.68 | 22.8 | 5.3 |
| EMEA | 0.73 | 18.0 | 3.1 |
| LATAM | 0.66 | 32.8 | 2.1 |

**NEARLY ALL INDUSTRIES RESPOND TO HACKERS IN LESS THAN ONE DAY.**

# CONTINUOUS DEVELOPMENT NEEDS CONTINUOUS SECURITY

**CONTINUOUS INTEGRATION AND CONTINUOUS DELIVERY** have become the new benchmark for DevOps teams. Applications are delivered faster, code changes are automatically pushed into production, and teams are developing in-house apps without external feedback. The speed of development now matches the speed of innovation.

This fast pace and frequent release cycles, coupled with emerging languages, has kept CISOs on their toes as companies grow and corners are cut to get releases out  the door. It's also pushed more teams to "shift left" on their security efforts: improving coding practices, identifying and eliminating vulnerabilities during development, and reducing risk as code moves into production.

**THE BEST COMPLEMENT FOR CONTINUOUS DEVELOPMENT IS CONTINUOUS SECURITY.**

While building security into your software development lifecycle (SDLC) without slowing down development is a challenge, hacker-powered security can help. Bug bounty programs empower companies to build a more security-aware engineering team who can work to close gaps before they're released.

By pushing security and vulnerability intelligence to the left in a SDLC, continuous security helps protect future releases against threats. It prevents new products and applications from going into production with vulnerabilities. And it maximizes bounty program value to the organization and reduces the risk of future breaches. In other words, the same vulnerability reports used to drive improvements in your software production process can also ensure future code is continuously more secure. Ship code, not bugs.

As organizations begin a bounty program, they rightly focus on fine tuning the basic bugs in, bugs out process. When welcoming outside hackers into your security operations is still new, there is a lot to get right—things like effective communications with hackers, triage, reproducing reported vulnerabilities, severity classification, bounty amounts, resolution process, and more. HackerOne has multiple resources available to help, from guides to our expert professional services team.

Read how Verizon Media used a bug bounty program to "shift left" in the SDLC.

# SECURITY IS NOT A ONE-TIME THING, BUT A CONTINUOUS CYCLE.

*"We know that there are always going to be bugs in software development. As we develop, and as we iterate, we want to make sure security is an active part of that process, and never a roadblock to innovation. The HackerOne bug bounty program allows us to put another cog in the wheel of security."*

**PETE YAWORSKI**
Senior Application Security Engineer, Shopify

+ + + + +

# BOUNTY TRENDS

## BY VULNERABILITY SEVERITY AND TYPE

By studying the trends and statistics of vulnerability reports, organizations can better prepare security and engineering teams for incoming report submissions. Benchmarking against industry standards also helps improve everyone's vulnerability disclosure and bug bounty programs. And, looking at trends on severity classifications and vulnerability types helps organizations, and the community as a whole, understand shifting areas of risk and prioritization.

Median value paid for critical vulnerabilities on HackerOne

**$2,500**

Average bounty paid for critical vulnerabilities on HackerOne

**$3,650**

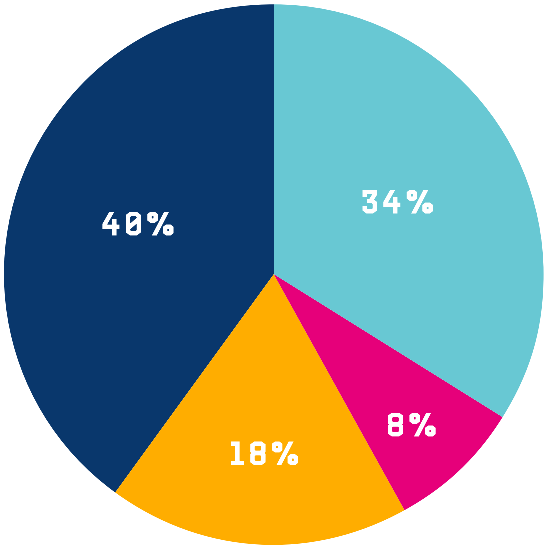
Incoming vulnerability reports are categorized by the vulnerability type and severity. To determine the type, HackerOne uses a vulnerability taxonomy mapped to the industry standard Common Weakness Enumeration (CWE). For severity, HackerOne uses the Common Vulnerability Scoring System (CVSS), an industry standard calculator used to determine bug severity. The hacker can either choose a severity level based on their own judgment, or they can use the CVSS.

Although customers themselves set bounty tables, HackerOne offers recommendations and insights, similar to this report, to help organizations benchmark their offered bounties against similar companies . Severity is particularly useful for structuring bounty ranges. When combined with the vulnerability type, this information streamlines the resolution process, allowing teams to integrate vulnerability reports with existing bug tracking systems. It also helps set hacker expectations on potential report resolution and bounty payouts.

Critical vulnerabilities make up just 8% of all reports. Medium severity bugs account for 40%, while low severity (34%) and high severity (18%) make up the remainder.

The median value paid for critical vulnerabilities on HackerOne was $2,500 / €2,120 / ¥17,400, which is up 25% from the 2019 median of $2,000, and double the $1,250 median of 2017. Critical vulnerabilities carry the most potential risk, so bounty values are generally much higher. The median value of a critical bug bounty is 2.5 -times that of a bug of high severity, and more than 6-times that for a bug of medium severity. As organizations fix more vulnerabilities and harden their attack surface, bounty values naturally increase over time, since vulnerabilities become more difficult to identify, thus requiring more skill and effort to discover.

The average bounty paid for critical vulnerabilities across all industries on HackerOne rose to $3,650 / €3,100 / ¥25,460 in the past year, up from $3,384 in 2019, $2,281 in 2017, and $1,977 in 2016.



## VULNERABILITIES BY SEVERITY

**Figure 7:** Percentage of vulnerabilities categorized by critical, high, medium, or low severity. Data from 2018-2019.

## MEDIAN BOUNTY VALUE BY SEVERITY

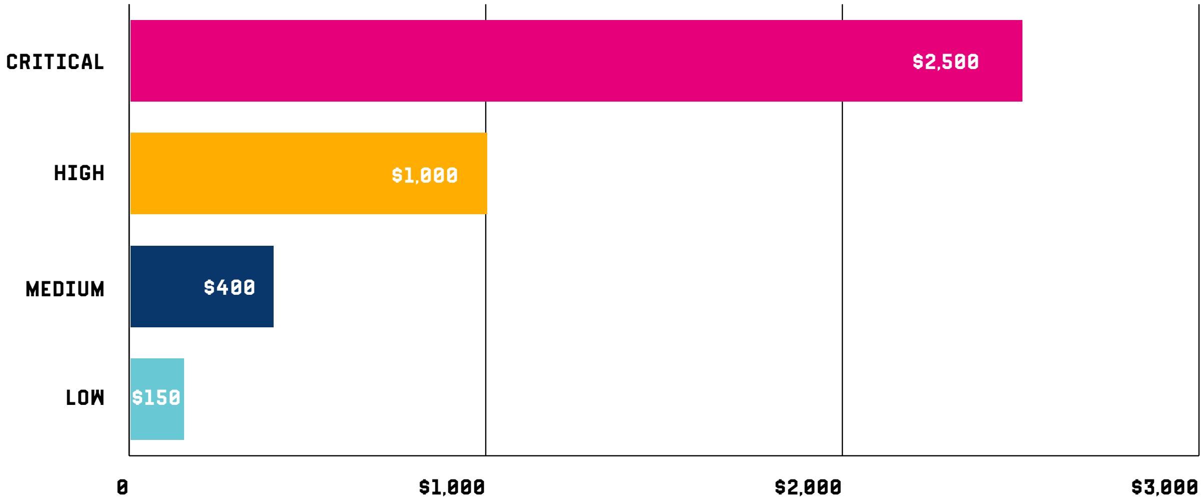


Figure 8: Median bounty values by severity.

## AVERAGE BOUNTY FOR CRITICAL VULNERABILITIES OVER TIME

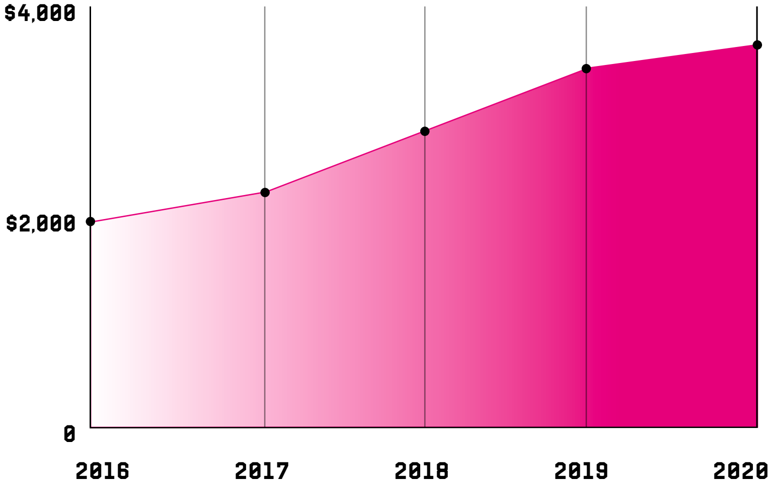
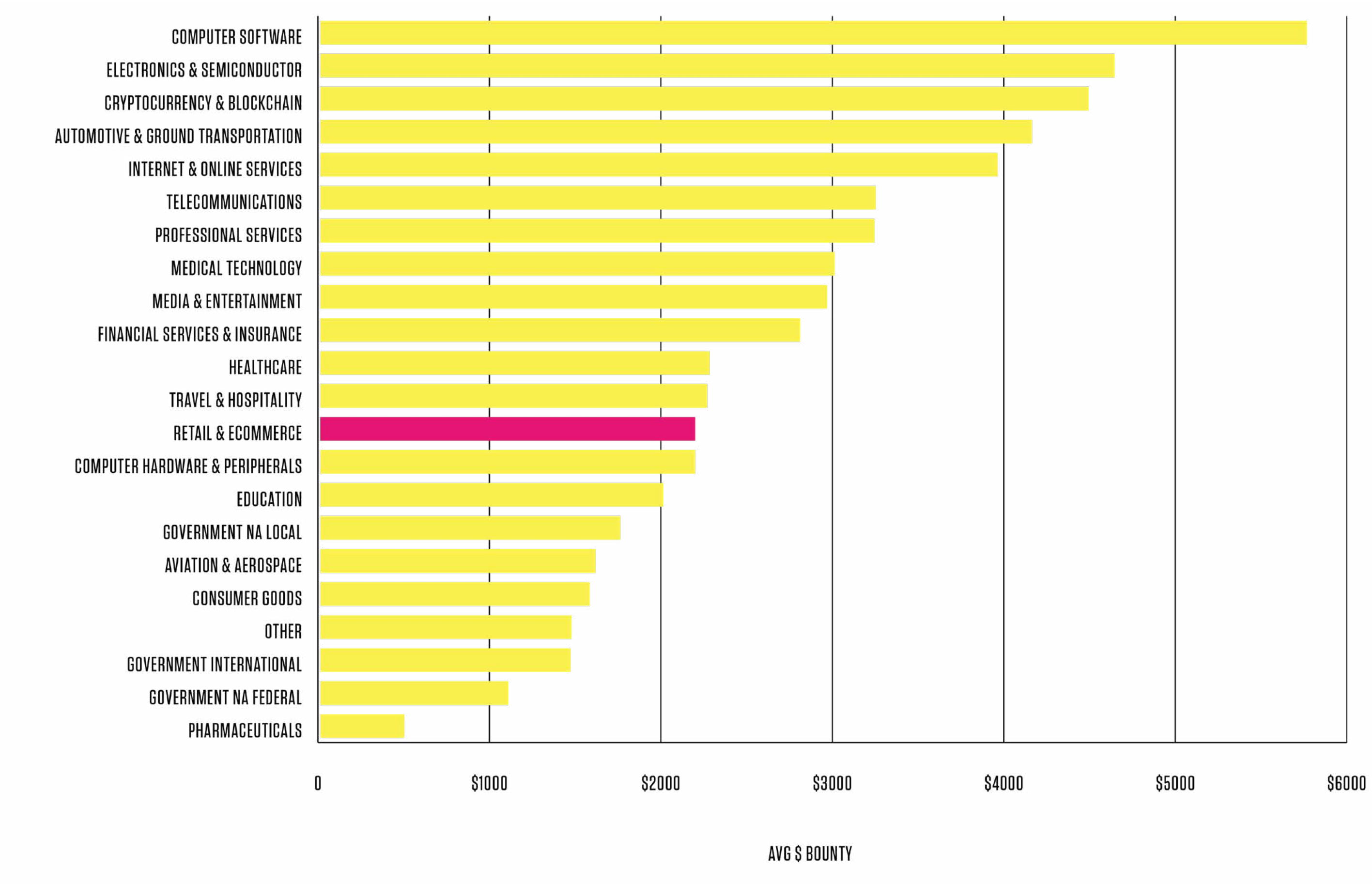


Figure 9: Average bounty values for critical vulnerabilities over time.

THE MEDIAN VALUE OF A CRITICAL BUG BOUNTY IS 2.5X HIGHER THAN A BUG OF HIGH SEVERITY, AND MORE THAN 6X HIGHER THAN A BUG OF MEDIUM SEVERITY.

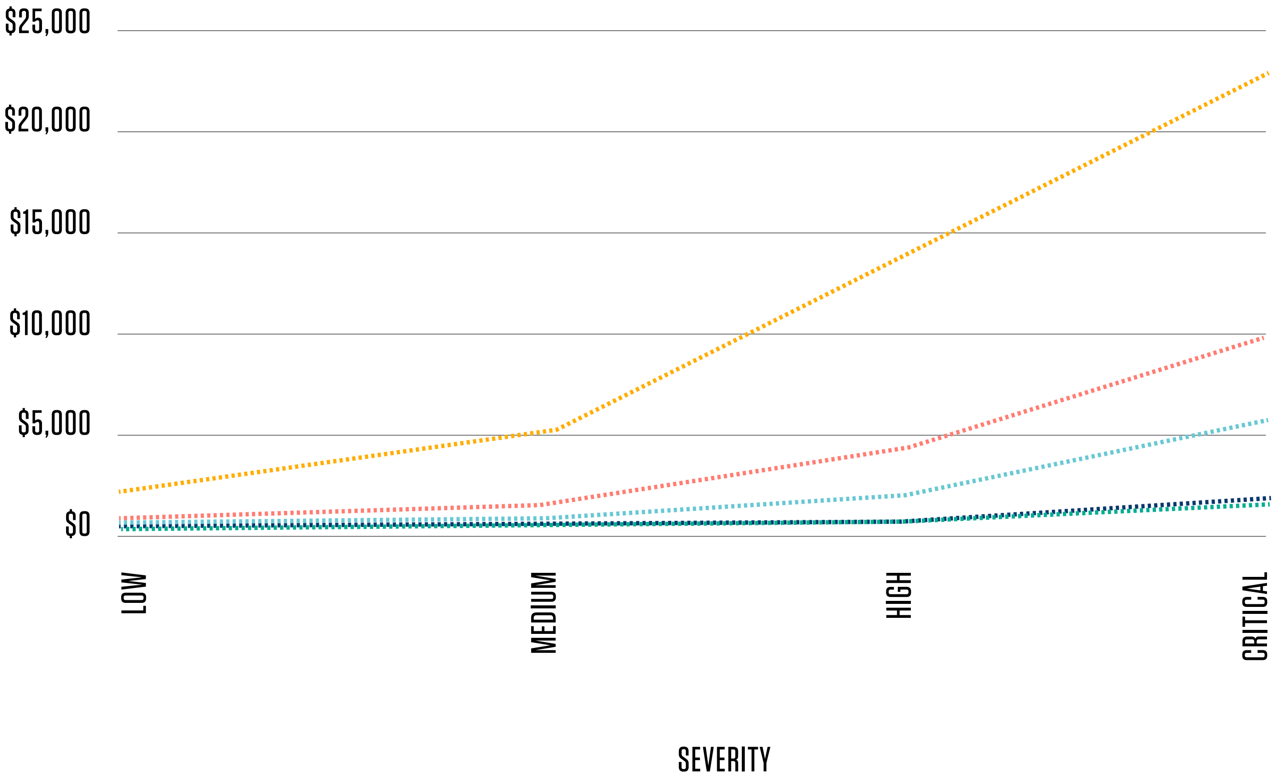
# AVERAGE BOUNTY PAYOUT PER INDUSTRY FOR CRITICAL VULNERABILITIES



Retail & e-commerce firms don't typically pay out the highest awards, the average pay out for a critical bug for this industry is $2,186. The highest average bounty payments by industry for critical issues come from Computer Software ($5,754), Electronics & Semiconductor ($4,663), and Cryptocurrency & Blockchain ($4,481). Those are all significantly higher than the platform average of $3,650. For all vulnerabilities reported of any severity, the average bounty payout was $1,024, up 33% from $771 last year, and up 119% from $467 in 2017.

**Figure 10:** Average bounty paid for critical vulnerabilities, by industry.

# AVERAGE BOUNTY PAYOUT BY SEVERITY



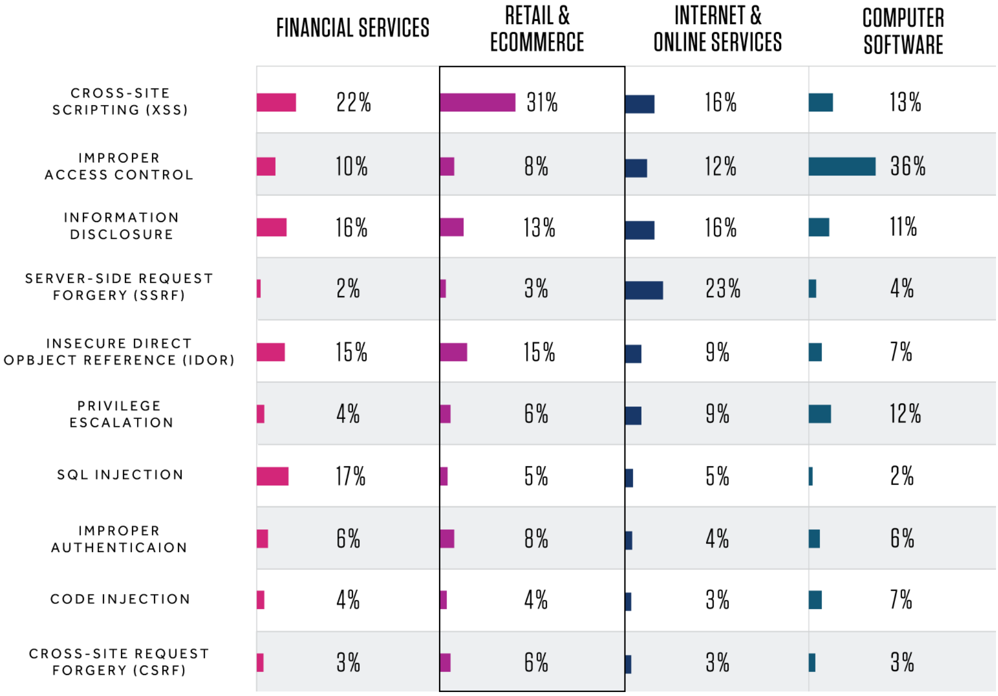
The average amount paid per vulnerability of any severity level is $979 / €831 / ¥6,834, which increased by 9% from last year's average. That's a small price to pay compared with the legal, brand, and engineering impact of a security breach, which the Ponemon Institute and IBM Security estimates at an average cost of nearly $4 million.

● 50TH PERCENTILE
● 60TH PERCENTILE
● 80TH PERCENTILE
● 90TH PERCENTILE
● 99TH PERCENTILE

**Figure 11:** Average bounty payout by severity.

# TOP VULNERABILITIES BY INDUSTRY

## (BY PERCENTAGE)



| | FINANCIAL SERVICES | RETAIL & ECOMMERCE | INTERNET & ONLINE SERVICES | COMPUTER SOFTWARE |
|---|---|---|---|---|
| CROSS-SITE SCRIPTING (XSS) | 22% | 31% | 16% | 13% |
| IMPROPER ACCESS CONTROL | 10% | 8% | 12% | 36% |
| INFORMATION DISCLOSURE | 16% | 13% | 16% | 11% |
| SERVER-SIDE REQUEST FORGERY (SSRF) | 2% | 3% | 23% | 4% |
| INSECURE DIRECT OPBJECT REFERENCE (IDOR) | 15% | 15% | 9% | 7% |
| PRIVILEGE ESCALATION | 4% | 6% | 9% | 12% |
| SQL INJECTION | 17% | 5% | 5% | 2% |
| IMPROPER AUTHENTICAION | 6% | 8% | 4% | 6% |
| CODE INJECTION | 4% | 4% | 3% | 7% |
| CROSS-SITE REQUEST FORGERY (CSRF) | 3% | 6% | 3% | 3% |

Of the top 10 most impactful and rewarded vulnerability types on HackerOne, cross-site scripting (XSS) vulnerabilities are the most common for retail & ecommerce organizations, making up 31% of total vulnerabilities surfaced, compared against 13% for computer software businesses. Insecure Direct Object Reference (IDOR) are the next most common for the sector but don't tend to pay out such high bounties, with the average payment for these vulnerabilities being just over $1000.

# TOP VULNERABILITIES BY INDUSTRY

## (TOTAL BOUNTY VALUE)

| | FINANCIAL SERVICES | RETAIL & ECOMMERCE | INTERNET & ONLINE SERVICES | COMPUTER SOFTWARE |
|---|---|---|---|---|
| CROSS-SITE SCRIPTING (XSS) | $344,093 | $208,200 | $1,748,557 | $645,437 |
| IMPROPER ACCESS CONTROL | $158,625 | $55,550 | $1,297,351 | $1,834,811 |
| INFORMATION DISCLOSURE | $242,313 | $90,625 | $1,712,707 | $583,876 |
| SERVER-SIDE REQUEST FORGERY (SSRF) | $30,000 | $17,250 | $2,452,591 | $192,207 |
| INSECURE DIRECT OPBJECT REFERENCE (IDOR) | $239,325 | $102,475 | $969,476 | $355,909 |
| PRIVILEGE ESCALATION | $65,915 | $41,685 | $988,539 | $640,451 |
| SQL INJECTION | $270,815 | $35,150 | $486,225 | $87,833 |
| IMPROPER AUTHENTICAION | $100,105 | $54,845 | $402,065 | $328,764 |
| CODE INJECTION | $62,398 | $28,430 | $274,610 | $342,375 |
| CROSS-SITE REQUEST FORGERY (CSRF) | $46,798 | $40,145 | $309,921 | $136,871 |
| TOTAL | $1,560,387 | $674,355 | $10,642,042 | $5,148,534 |

Find out more about the key takeaways of this data on our Top 10 website:
https://www.hackerone.com/top-ten-vulnerabilities

# WHO ARE THE HACKERS AND WHY DO THEY HACK?

Hackers are young, curious, and creative. Most (87%) hackers are under age 35 and 84% are self-taught. Just over half (53%) get at least half of their income from hacking, with 22% naming hacking as their only source of income. Just 53% do it for the money, with 68% saying their main motivation is that they enjoy the challenge of hacking. It's also a good career booster; 44% say they hack to advance their career and 80% say they've used, or plan to use, skills and experience learned while hacking to land a job. There's also an altruistic angle to hacking: 29% hack to protect and defend and 27% hack to do good in the world.

## HOW MANY YEARS HAVE YOU BEEN HACKING?

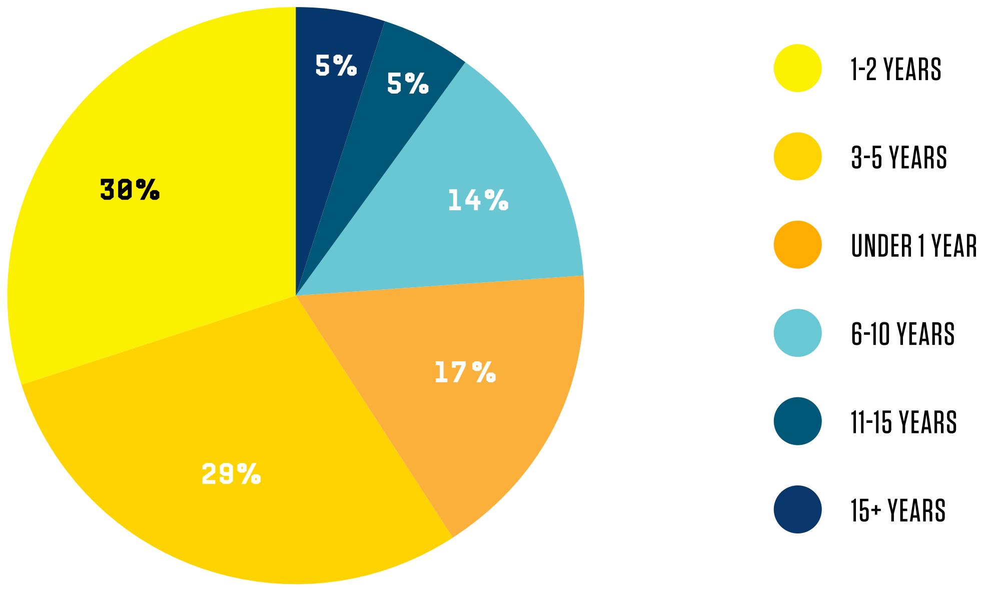


**Figure 14:** How long have you been hacking?

Hackers test your system in many more different ways than any one security contractor could afford to do. Every single model, every single tool, every single scanner has slightly different strengths, but also different blind spots. Every hacker brings a slightly different methodology and a slightly different toolset to the problem. Although automated tools for detection have gotten very good at flagging things that might be a problem, almost all of them are plagued with false positives that still require a human to go through and assess (if) it's actually a vulnerability. While automation can handle the grunt work, we still need skilled human eyes to see problems and solutions that computers can't. And, the earlier in the process you have hackers engaged, the better off you will be.

**TO LEARN MORE ABOUT THE HACKER COMMUNITY, WHY THEY HACK, HOW THEY LEARN, AND EVEN WHAT THEY DO WITH THEIR EARNINGS, DOWNLOAD THE 2020 HACKER REPORT.**

## FAVORITE PLATFORM TO HACK

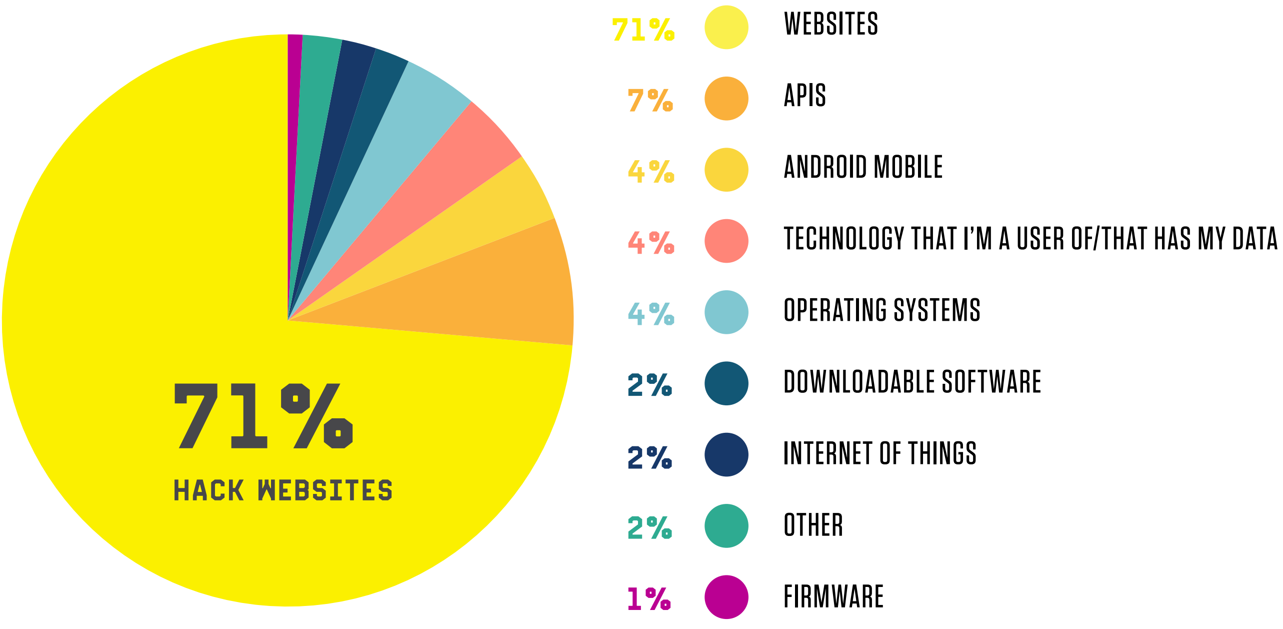


**Figure 15:** Favorite platforms to hack

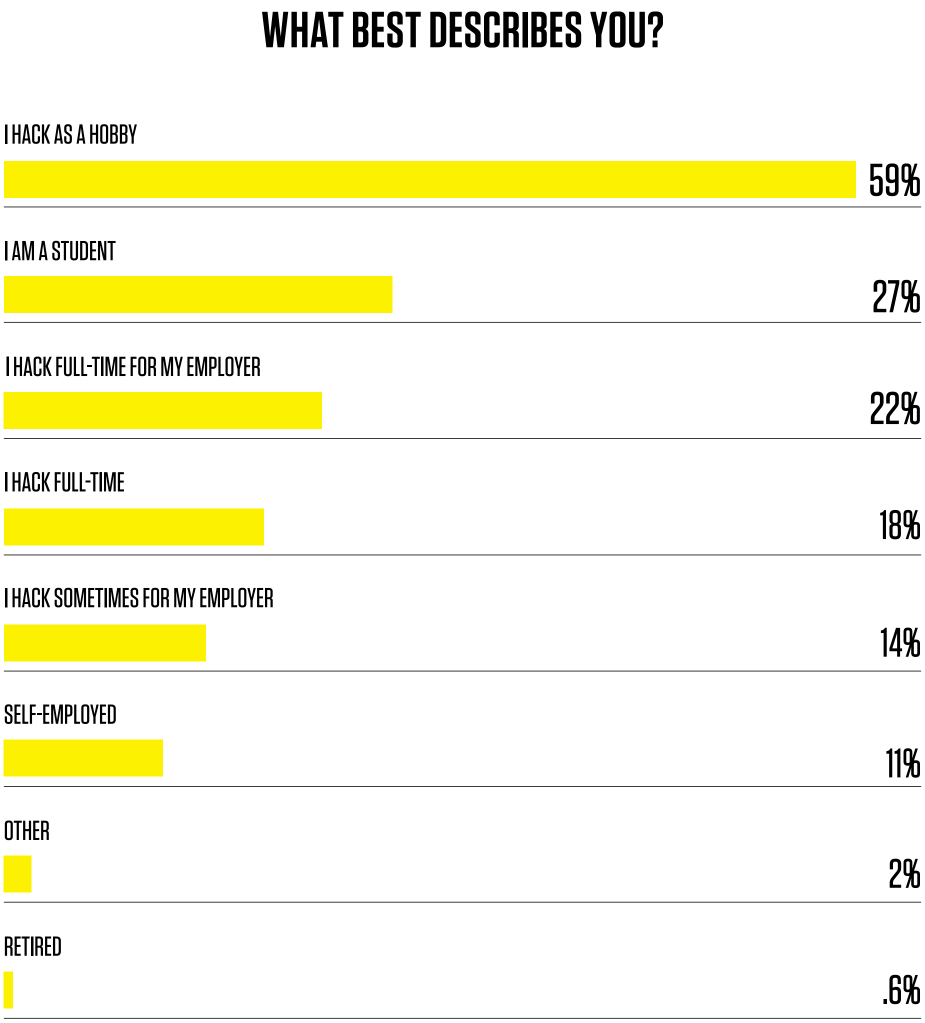


**Figure 16:** What best describes you?

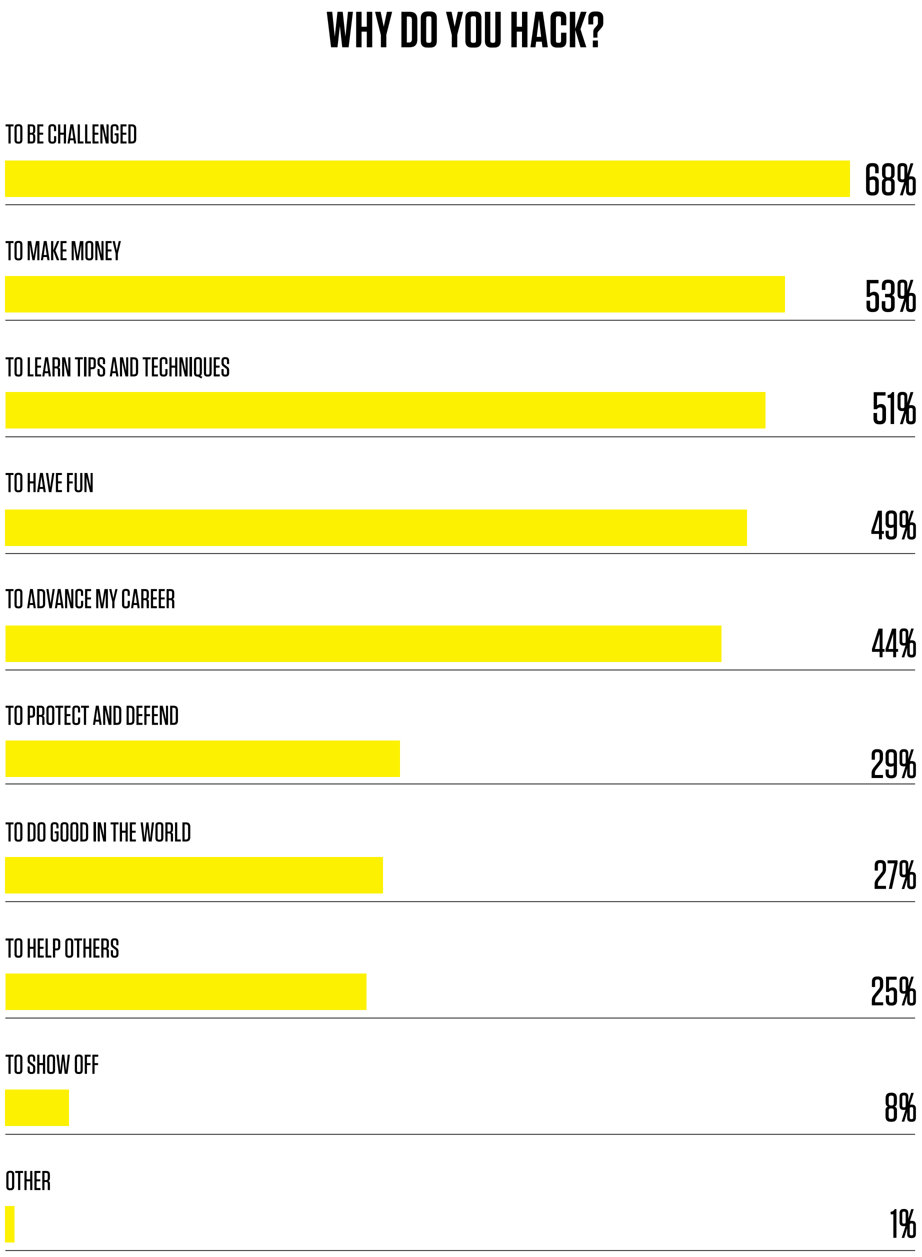


**Figure 17:** Why do you hack?

## EUGENE

**@SPACERACOON**

*"I am motivated by the thrill of finding a bug and learning something new. Every time I read an article on new exploitations or discovery techniques, I'm itching to try it out. I love thinking of clever ways to bypass a defense or apply a novel attack."*

## TOM

**@TOMNOMNOM**

*"It's a lifelong obsession with how things work. There's this great Richard Feinman quote, which is: 'What I cannot create, I do not understand.' And I think, for software, you've got to apply an additional layer of 'What I cannot break, I do not understand.'"*

## KATIE

**@INSIDER_PHD**

*"The community is super encouraging. The community is super willing to help out. It's, as far as I'm concerned, my home."*

## ALYSSA

**@ALYSSA_HERRERA**

*"What motivates me is wanting to help out security companies protect against breaches and improve their general security. Another motivation is being a role model for other women who also might want to get into this field of work."*

## ALEX

**@AJXCHAPMAN**

*"I like the challenge. I like the variety that hacking gives and the opportunity for continued learning. It's a really good way of proving yourself and extending your knowledge every day."*

## BEN

**@NAHAMSEC**

*"The one skill hackers must inherently have is the ability to problem solve and a strong sense of curiosity around how technology works and how it could possibly fail us."*

# CLOSING THOUGHTS

**HACKER-POWERED SECURITY IS THE FUTURE OF CYBERSECURITY — AND THAT FUTURE IS HERE**.
In an era of increasing uncertainty and unprecedented challenges, hackers are empowering organizations to keep their customers safe: in more areas of the world, on more attack surfaces, in new ways, using new tools and methods. Security leaders are partnering with hackers to supplement their security teams, reduce risk across the software development lifecycle, achieve compliance, and reinforce brand trust.

And hackers — these creative individuals who enjoy overcoming limitations -- are using this partnership to support themselves and enrich their communities. Hackers have already received over $100 million / €85 million / ¥696 million in bounties. And we estimate that total to grow by 1,000% within the next 5 years. Many hackers are donating their bounties to charitable causes.

The COVID-19 pandemic has shown us how small and interconnected our world is. Technology is fundamentally global, and yet the systems upon which we have built our digital lives can be upended in seconds. We rely on these systems for everything: to work, live, learn, travel, to buy and sell things, to experience art and entertainment. To threaten these systems is to threaten our way of life.

But this interconnectedness is a positive thing, too. Keeping the internet safe is a global effort. Finding the hundreds of millions of vulnerabilities in our technology would be impossible without an international pool of talent.

Hackers know that. Security leaders know that. Boards are starting to mandate it; government agencies are recommending it as a best practice. And HackerOne is here to lead the charge.

TOGETHER, WE HIT HARDER — AND AS A GLOBAL COMMUNITY, WE HACK FOR GOOD.

# METHODOLOGY & SOURCES

Findings in this report were collected from the HackerOne platform using HackerOne's proprietary data based on over 2,000 collective bug bounty and vulnerability disclosure programs. The 2020 data in this report spans from May 2019 through April 2020.

**FORBES GLOBAL 2000 VULNERABILITY DISCLOSURE RESEARCH:** Our research team searched the internet looking for ways a friendly hacker could contact these 2,000 companies to disclose a vulnerability. The team looked for web pages detailing vulnerability disclosure programs as well as email addresses or any direction that would help a researcher disclose a bug. If they could not find a way for researchers to contact the company to disclose a potential security vulnerability, they were classified as not having 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.

**COVID CONFESSIONS OF A CISO:** Research conducted by Opinion Matters on behalf of HackerOne. The survey includes responses from 1,400 security professionals in companies employing 1,000 or more, and located in the U.K., France, Germany, Australia, Singapore, the U.S.A. and Canada. Research was conducted in July 2020.

**THE 2020 HACKER REPORT:** Data was collected from a proprietary HackerOne survey in December 2019 and January 2020, totaling over 3,150 respondents from over 120 countries and territories. The surveyed individuals have all successfully reported one or more valid security vulnerabilities on HackerOne, as indicated by the organization that received the vulnerability report.

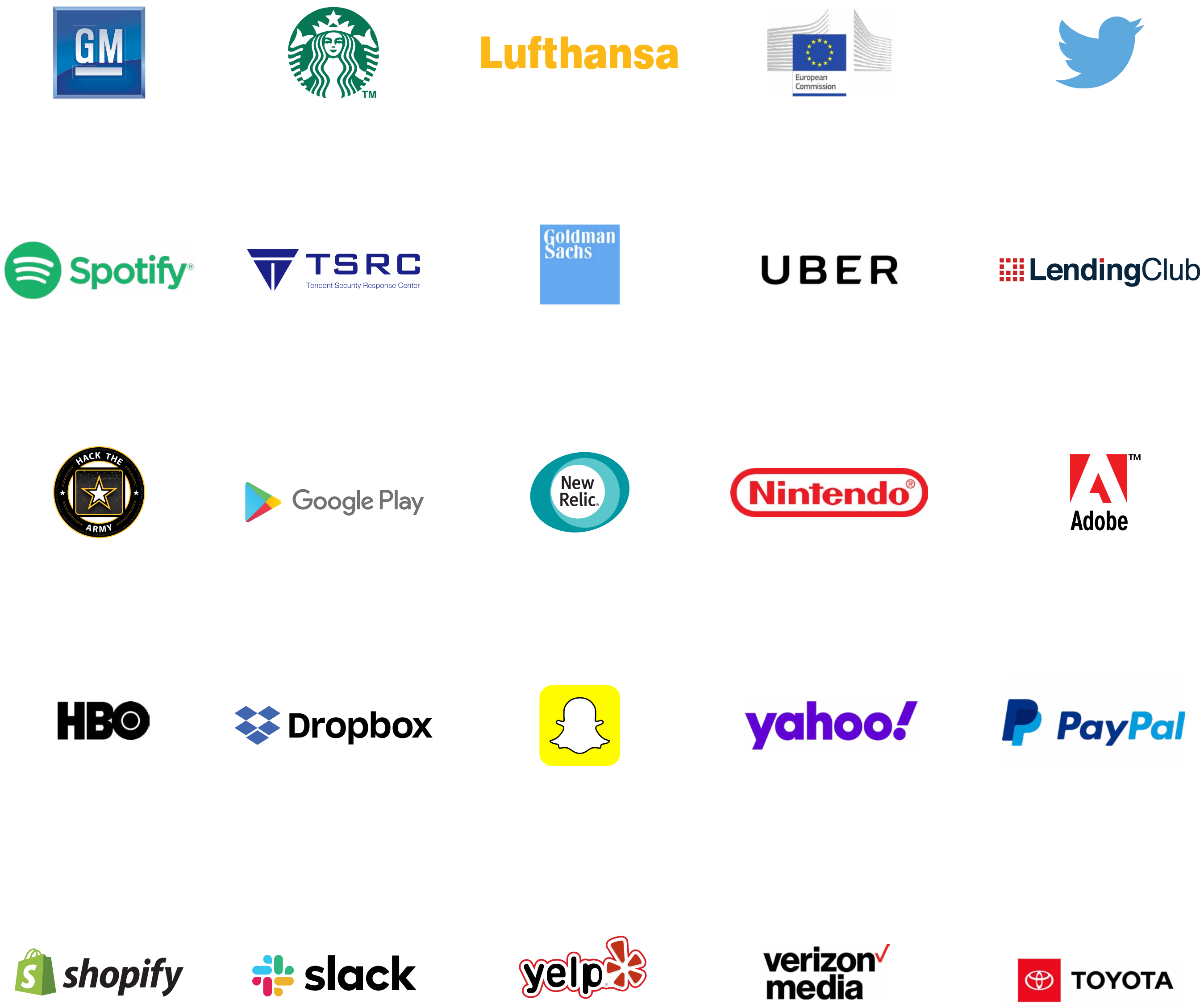
# ABOUT HACKERONE

**HACKERONE EMPOWERS THE WORLD TO BUILD A SAFER INTERNET.** As the world's trusted hacker-powered security platform, HackerOne gives organizations access to the largest community of hackers on the planet. Armed with the most robust database of vulnerability trends and industry benchmarks, the hacker community mitigates cyber risk by searching, finding, and safely reporting real-world security weaknesses for organizations across all industries and attack surfaces.

Customers include The U.S. Department of Defense, Dropbox, General Motors, GitHub, Goldman Sachs, Google, Hyatt, Intel, Lufthansa, Microsoft, MINDEF Singapore, Nintendo, PayPal, Qualcomm, Slack, Starbucks, Twitter, and Verizon Media. HackerOne was ranked fifth on the Fast Company World's Most Innovative Companies list for 2020. Headquartered in San Francisco, HackerOne has a presence in London, New York, the Netherlands, France, Singapore, and over 70 other locations across the globe.

# TRUSTED BY

MORE FORTUNE 500 AND FORBES GLOBAL 1000 COMPANIES THAN ANY OTHER HACKER-POWERED SECURITY ALTERNATIVE.



THE WORLD'S MOST TRUSTED HACKER-POWERED SECURITY PLATFORM

hackerone