PRIORITY ONE

A NEW DECADE IN Crowdsourced Cybersecurity

bugcrowd

TABLE OF CONTENTS

INTRODUCTION

EXECUTIVE SUMMARY

Upheaval, uncertainty, and change defined 2020 in the cybersecurity sector and beyond. As the pandemic wreaked havoc on the global economy, malicious actors sought to capitalize on the circumstances. The World Health Organization reported that attacks **increased by 500%** soon after the pandemic began, driven by a **sevenfold increase in Ransomware** and the new attack vectors that open up in a remote-first world of work.

Against this backdrop, there was also massive growth in crowdsourced security. Companies are investing more in the use of ethical hackers to identify vulnerabilities and bugs in their assets, getting ahead of the bad guys by crowdsourcing expertise from the white hat community. **The new threat landscape is leading to a business boom for locksmiths, not just for burglars.**

KEY FINDINGS

- **50%** Increase in submissions
- **15-20%** Growth in total payouts per quarter
- **65%** Increase in P1 submissions (most critical vulnerabilities)
- **4%** Increase in validity of submissions
- **2x** Submissions for APIs
- **3x** Submissions for IoT
- **2** New entries in the top ten vulnerability categories
- **3x** Software P1 submissions

As well as growth in submissions and payouts, the sector has matured on both the supply and demand side. Ethical hackers are chaining bugs together and developing proof of concepts to find more critical vulnerabilities. Buyers are recognizing the power of the hacking community, the Crowd, and integrating them more deeply into their Security Development Lifecycle through source code analysis and increased integration of the Bugcrowd platform.

The last year shows us a sector that is maturing and reaching the next level of sophistication. Security researchers are maturing and becoming more entrepreneurial and professional, building and developing more tools while wrestling with emerging government support on one hand and legal risk on the other. Early adopters of techniques such as recon and scanning benefited greatly, creating millionaire hunters and bringing this approach into the mainstream, while improved resources and ever-present human error ensures that the industry remains open and welcoming to novices.

It has been a transformational year for crowdsourced security, with big implications for the next decade of the industry. Let's take a closer look.

METHODOLOGY

This report draws from proprietary data taken from Bugcrowd's platform, supplemented by dozens of hours of interviews with hackers discussing their hunting strategies, industry insights, and outlooks for the market as a whole. It is data-driven and positioned within a fast-moving industry during a time of considerable change and innovation. By taking a broad lens to the industry, it demonstrates the growing role of crowdsourced security.

CROWDSOURCED SECURITY TODAY

INCREASED ADOPTION

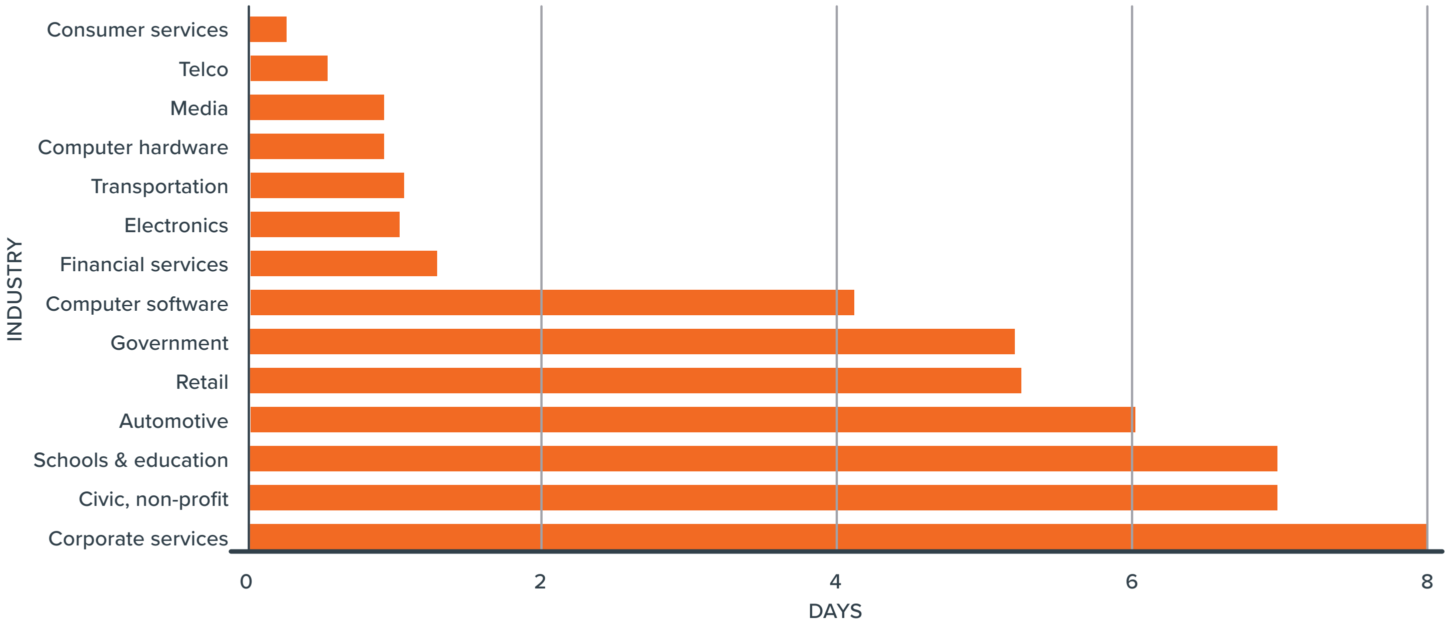
When we talk about crowdsourced security, we are talking about human potential. Throughout history, there have always been barriers to commercial innovation, from medieval guilds to protectionist regulation. Much of this rightly centered around safety, ensuring a high quality of work, but some did nothing more than exclude talented and hardworking individuals from reaching their potential and contributing economically. History is filled with examples of large populations excluded from the research, innovation, and practices that define the world they lived in.

This has changed rapidly in the recent past. The internet allows us to unlock human potential like never before, offering billions of people around the world the chance to educate themselves and create value. Nowhere is this opportunity more obvious than in **security, the purest meritocracy in the digital world.**

Our industry has taken software testing and penetration testing, historically closed shops that were hard to access, and opened them to everyone with an internet connection. Hackers from all over the world are able to create crowdsourced security profiles and get to work finding bugs and making money, **improving global security standards** in the process.

For almost all industries, crowdsourced security **reveals vulnerabilities in a matter of days, or even hours.** Sectors that are more familiar to the public like consumer services and media see their first critical vulnerabilities in less than a day. Government and automotive will take a few days, but vulnerabilities in these industries will often represent far higher stakes. Speed of discovery across the board shows that crowdsourced security can always add value to security teams.

AVERAGE DAYS TO FIRST CRITICAL OR HIGH PRIORITY VULNERABILITY



Hackers are finding **more bugs** with **greater accuracy.**

Data reveals that the crowdsourced security sector continues to grow at a rapid pace. Bugcrowd received **50% more submissions in the last 12 months than the year prior.** Throughout this period, there was a **65% increase in P1 submissions**, the most critical vulnerabilities, and overall submission quality improved as the **validity of vulnerabilities increased by 4%**. Hackers are finding more bugs with greater accuracy. Web apps are still responsible for the majority of vulnerabilities, but other categories are gaining ground as hackers diversify their skill sets to stay competitive in an increasingly competitive space. In the last year, Bugcrowd saw submissions to all targets increase, though notably **API vulnerabilities doubled**, while those found in **Android targets more than tripled.**

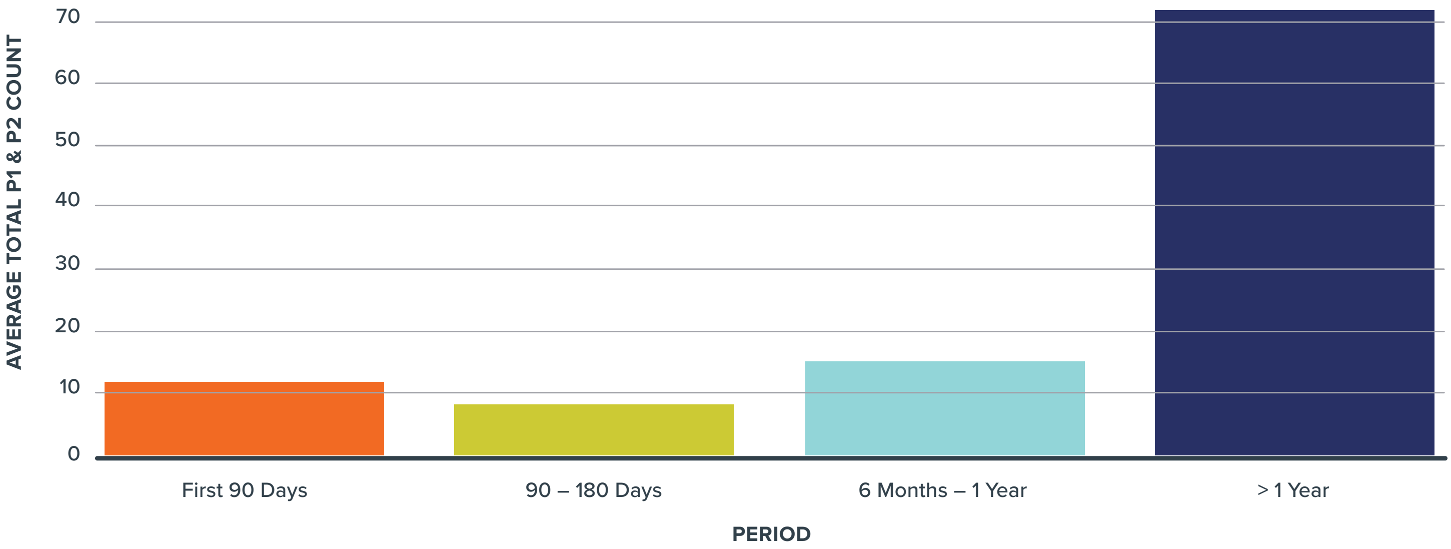
Changes to crowdsourced security arising from the pandemic were most concentrated in the software sector, where submissions in 2020's first ten months already outstripped all of 2019, **up 24% in total submissions.** But what was most impressive was the jump in quality of submissions during this time, with **P1 submissions almost tripling** in the shorter time period. The number of duplicate submissions also increased, indicating that the **competition for software bugs is rising.**

The financial services sector was also significantly impacted, returning more submissions from January to October of 2020 than in all of 2019. **The pandemic caused buyers in this sector to double their payouts for P1 vulnerabilities from Q1 of 2020 to Q2.** Automotive and hardware bugs were down in 2020, as new working conditions did away with the bug bashes that normally provide the majority of the bugs submitted in these sectors.

Comparing data from the last two years shows a sector that is maturing, with increasing competition. Submissions are up, with higher numbers of critical vulnerabilities and more duplicates, while total payouts are growing steadily by about 15-20% per quarter. Buyers are seeing more bang for their buck as higher investment leads to more critical vulnerabilities being found, and hackers are innovating faster while taking advantage of a growing market. There is also evidence of crowdsourced security becoming an integral component of the security lifecycle, with the number of critical submissions discovered in the first year of a program just a fraction of those discovered in the following years.

Buyers are seeing more bang for their buck as **higher investment** leads to **more critical vulnerabilities being found**, and hackers are innovating faster while taking advantage of a growing market.

P1 & P2 BREAKDOWN BY PERIOD



1

2019
Cross-Site Scripting (XSS) → Reflected → Non-Self

2020
Broken Access Control (IDOR) → Broken Access Control

2

2019
Broken Access Control (IDOR) → Broken Access Control

2020
Cross Site Scripting XSS (Reflected) → Non-Self

5

2019
Cross Site Scripting XSS (Stored) → Non Admin to Anyone

2020
Server Security Misconfiguration → Misconfigured DNS → High Impact Subdomain Takeover

6

2019
Unvalidated Redirects and Forwards → Open Redirect → Get Based

2020
Cross Site Scripting XSS (Stored) → Non Admin to Anyone

9

2019
Broken Authentication & Session Management → Weak Login Function → HTTPS Not Available or HTTP by Default

2020
Sensitive Data Exposure → Critically Sensitive Data → Private API Keys

THE TOP TEN VULNERABILITIES

3

2019
Sensitive Data Exposure → Critically Sensitive Data → Password Disclosure

2020
Broken Authentication & Session Management → Privilege Escalation

4

2019
Broken Authentication & Session Management → Privilege Escalation

2020
Cross Site Scripting XSS (Stored) → Privileged User to Privilege Elevation

7

2019
Server Security Misconfiguration → Misconfigured DNS → High Impact Subdomain Takeover

2020
Unvalidated Redirects & Forwards → Open Redirect → Get Based

8

2019
Broken Authentication & Session Management → Authentication Bypass

2020
Broken Authentication & Session Management → Authentication Bypass

10

2019
Sensitive Data Exposure → Critically Sensitive Data → Private API Keys

2020
Server Side Injection → Remote Code Execution (RCE)

*Due to a revised methodology, the 2019 top ten bugs differs slightly from the version published in last year's Priority One report.

While the world's economic, technological, and political structures are in flux, some things in security never change. The top 10 bugs submitted by **Vulnerability Taxonomy Rating (VRT)** saw eight of last year's top ten repeated this year, showing that a lot of security comes down to getting on top of known risks. Even though security remains on the cutting edge of technology, we continue to see the industry confronting repeated and avoidable errors.

Privilege elevation is a new entrant at number four, which could be an indication that security researchers are working harder with their vulnerabilities to build proof of concepts that can raise the severity of the bugs they find, increasing their rewards in the process. This indicates the sector is maturing, as **hackers raise the bar on their submissions and buyers get more results for their investment**, relieving the workload of their in-house teams.

Even though security remains on the cutting edge of technology, we continue to see the industry **confronting repeated and avoidable errors.**

The changes in the top 10 also reflect crowdsourced security trends of 2020, such as the increased use of automated recon and scanning. Subdomain takeovers rose two places from sixth to fourth, driven by increased use of automation and hunters developing advanced recon techniques. But this does not mean scanning is becoming compulsory for bug hunting. **Broken access controls rose to become the most submitted vulnerability in 2020**, ahead of cross-site scripting. This vulnerability is driven by human error, replacing last year's top vulnerability, which could be caught by the correct use of frameworks. Bugcrowd research found that **78% of hackers predict they will be able to outsmart AI for the next decade.** We see that humans will always be a source of security risk, and hunters who recognize this and capitalize on it will be in high demand.

When assessing an organization's security landscape, organizations should not only look at prevalence of vulnerabilities, but also the **creativity of the participants themselves.** Hackers who can chain together multiple vulnerabilities can identify risk and improve security at a higher level of abstraction. As scanner technology and AI becomes more sophisticated, **this ingenuity represents the enduring value of the Crowd.**

A GLOBAL PANDEMIC: NEW CHALLENGES AND OPPORTUNITIES

The coronavirus pandemic rocked the world economy in 2020, confining knowledge workers to their homes and overhauling the priorities of IT and security teams. Initially, the security industry focused on keeping the lights on, with management often stressing availability above the other parts of the CIA triad. Security professionals had to grapple with the **immediate impact of changing work practices** as well as the second-order effects of stalled plans and revised priorities.

Challenge
Government lockdowns and quarantine periods mean more time spent indoors or at home.

Opportunity
This led to an increase in time spent on the platform, causing higher activity and more results. There was also an **increase in payouts for critical vulnerabilities as P1 payouts spiked by 31% from Q1 to Q2** in 2020. This trend was concentrated at the elite level, with P2 payouts seeing a delayed 31% bump between Q2 and Q3, while payouts for other categories remained static.

Challenge
Remote-first working led adversaries to adapt their tactics, with attack vectors now running right through living rooms and home offices. This led to a **spike in the black market values of home office exploits in equipment such as printers or routers.**

Opportunity
Hardware manufacturers responded by investing in testing and revisiting their crowdsourced security programs.

Challenge
Remote access vulnerabilities also became a more urgent consideration, as 2020 saw **increased uptake of the Pulse VPN bug** originally uncovered in **April 2019**, increasing risk of ransomware just before VPN usage shot up globally. The **F5 Bug** in July also attracted attention, creating the potential for remote code execution and lateral movement in software that was highly prevalent across internet infrastructure.

Opportunity
Bugcrowd hunters submitted F5 vulnerabilities before it was announced, raising the alarm on a vulnerability that had over 7,000 instances and led to a great deal of submissions.

HACKER-POWERED CONTENT

One positive result from the recent spotlight on security is the explosive growth in thought leadership content within the security industry. Hackers tend to be early adopters, and many began publishing security content on blogs, podcasts, videos, and streaming. Bugcrowd's virtual "Level Up" conference looked remarkably prescient when we hosted it in the remote-first world during August, and we saw a huge uptick in attendance and contributions as a result.

Growth in hacking as an industry also allows it to become more professional and polished, allowing many hackers to **build personal brands** for themselves. Some who started out as novices in the Crowd built up audiences and reputations, becoming thought leaders in a growing and vibrant industry. Bugcrowd research found that bug hunters skew younger than the rest of the security industry, and this may help to explain why there is so much content being produced by hunters across a number of platforms. **Video and streaming content** is becoming particularly popular, with new thought leaders popping up in 2020 and established ones increasing their output. This feeds into a general **trend of hunters becoming more entrepreneurial** and investing more in their personal brands.

FARAH HAWA

This up-and-coming bug hunter became a YouTube star in 2020 with her training videos and honest accounts of starting out as a novice in the industry. After posting her first video in late May of this year, Farah has gained a YouTube following of almost 14,000 subscribers for her videos, offering advice and support to junior hackers. Fans love the genuine content coming from someone who is also early on in her career, and her platform has allowed her to interview elite hackers such as Chloe Messdaghi, @Akita_Zen, and @ Th3G3ntl3man.

Farah started her career in 2018 doing pen tests, audits, and assisting her team with seminars and workshops for college students. In 2020, she started bug bounties. While she still sees security as her primary occupation, she also aspires to becoming the go-to resource for beginners learning web hacking techniques.

KATIE PAXTON-FEAR

While data suggests that many hackers are self-taught, having a degree in Computer Science, experience working as a data scientist, and studying for a PhD in Defence and Security certainly helps. Katie is living the hacker dream by bug-hunting while completing her studies, while also, somehow, finding time to become a content creator, amassing over 19,000 subscribers on YouTube in a year.

Although her knowledge base is deep, Katie still commits a lot of her time to creating tutorials and explanatory videos for beginners. This allows her to give back to the community, and to pursue her goal to be a security educator as well as a professional.

HEATH ADAMS (THE CYBER MENTOR)

Cyber polymath Heath's career includes pen testing, bug hunting, entrepreneurship, teaching, and running a nonprofit to help his fellow veterans find work in the sector. This makes his side-hustle as The Cyber Mentor, creating content for his more than 142,000 YouTube subscribers, all the more impressive. Heath uses digital channels to offer free videos and promote his cyber training courses, focusing on beginner and intermediate skills.

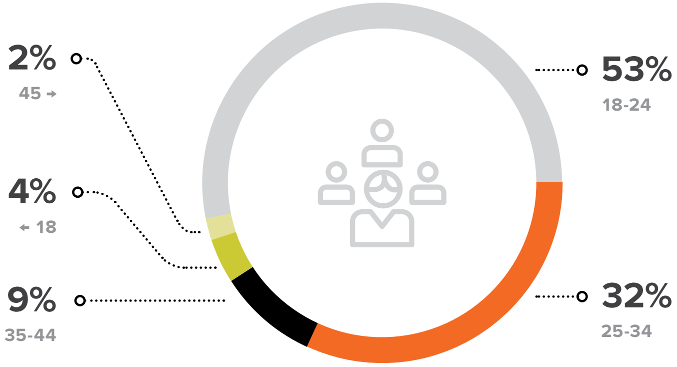
In 2020, The Cyber Mentor channel continued its impressive growth on YouTube, but it was on streaming platforms like Twitch where his viewership blew up during the pandemic, as numbers doubled and tripled in the second quarter. Heath attributes this to his younger audience being more native to video, as well as their preference for more visual content and shorter attention spans.

BUG HUNTERS: A COMMUNITY INVESTING IN THEIR CRAFT

A booming crowdsourced security market has increased competition and led hackers to work hard at developing their skill set and improving their knowledge. We know that diversity is hardwired into the Crowd—Inside the Mind of a Hacker showed that **elite hackers are more neurodiverse than the general population**—and now many are diversifying their experience and skills to remain competitive. Growth in demand for bounty programs in new areas such as APIs and IoT is incentivizing hackers to apply themselves to learning these technologies, as well as providing **starting points and opportunities** for those breaking into the industry.

Support and encouragement for novice hunters is the status quo for the Crowd. Security culture is a subset of internet culture, and still upholds several of the values that have been associated with this counterculture since the days of Usenet. These include meritocracy, community, and a willingness to invest time and resources in open-source resources. Just like those early adopters and trailblazers, **modern hackers are young, with 53% aged 18-24, and are often driven by a pronounced moral compass**. Most disregard lucrative financial rewards for vulnerabilities on the black and gray market in favor of applying their talents to improving security and dedicate some of their time to giving back to the community.

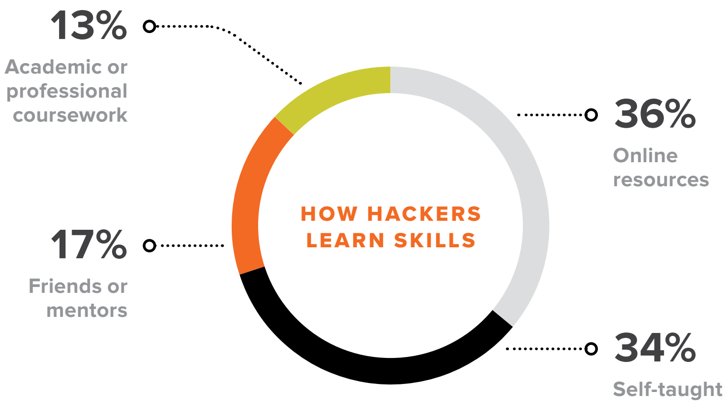
AVERAGE AGE OF HACKERS



> Keeping this inclusive culture ensures that the crowd remains diverse, vibrant, and meritocratic, adding to the utility of crowdsourced security in a rising tide that lifts all boats.

Security professionals have also seen a distinct shift in working, as Bugcrowd research found that **83% of security professionals expect to remain partially or fully remote indefinitely.** Less time spent commuting and in meetings means more efficient hunting, as seen by the rise in submissions and validity when many countries went into lockdown during the second quarter. Buyers of crowdsourced security also adapted their tactics, with **85% planning to prioritize remote testing over in-person alternatives** due to the new working conditions.

As interest in hacking continues to increase, hackers are building and publishing open-source tools along with detailed guidance and tutorials. Many hackers will keep a tool or technique private early on as a competitive advantage, but once these enter the mainstream, they will often publish techniques and make tools open source. Doing this ensures these tools benefit from greater community support for their upkeep, but it also means that junior hackers and the community as a whole benefit from the tool. Keeping this inclusive culture ensures that the crowd remains diverse, vibrant, and meritocratic, adding to the utility of crowdsourced security in a rising tide that lifts all boats.



> At the heart of the security sector is a thriving community built on support, mentoring, and friendship.

This process supports buyers by commoditizing hunting for vulnerabilities that are low complexity, driving experienced hunters to seek returns by going after more complex bugs or chaining vulnerabilities together for more lucrative rewards. **The ecosystem benefits because novice hackers are given the resources to learn their trade** while cutting their teeth on entry-level problems, while those with more experience can still earn money improving security. Some are even collaborating on entrepreneurial projects, similar to gold prospectors moving from panning in streams to building mining operations. **Rising standards** benefit buyers most of all and make it far tougher for bad guys.

While resources are improving through open-source education and democratization of tools, there are still some barriers remaining in the way of those looking to build a career in security.

In some circles, **a stigma remains around security research and education;** some continue to associate it with criminality. Short-sighted reactions have caused some individuals to call for bans on hacking resources and tools. This even extended to YouTube **taking down security research videos**, and led remote voting company Voatz to publicly call for restrictions on security research (more below). At the heart of the security sector is a thriving community built on support, mentoring, and friendship. Part of this proud tradition of supporting junior and inexperienced hackers is ensuring that free resources remain available and that money does not become a barrier to entry into the industry. This spirit informs Bugcrowd's own culture, as we are committed to making educational resources in **Bugcrowd University** freely available online to keep the industry as meritocratic as possible.

GROWTH OF RECON: THE NEW “OUTSIDE IN” APPROACH

Companies have been buying crowdsourced security solutions to work within a clearly defined scope for years now and have used pen tests to similar ends for decades before that. But as the industry blooms and competition increases, **positive externalities** emerge outside of these scopes.

Some organizations have opened up their bounty scope to include any assets that are demonstrably owned by them, taking advantage of **high competition and creativity within the Crowd.** Changes in scope combined with the first-to-find model of bug bounties drove hunters to use reconnaissance to find obscure and forgotten assets that buyers had been unaware of. **By uncovering shadow IT and unknown assets that were contributing to the company’s cyber risk, hunters identified a rich new seam of bugs and bounties.** These assets made for happy bug hunting, and security teams were impressed, and slightly concerned, when presented with the findings. The resulting concerns about shadow IT led to the addition of recon as a crowdsourced security solution in the form of **Attack Surface Management** (ASM).

Research conducted by the Enterprise Strategy Group shows that organizations with more mature security programs are more likely to acknowledge that their attack surfaces changed frequently, which leads to unknown assets with increased security risk.

Why does your organization perform attack surface management?	All Respondents	Leaders	Fast-Followers	Emerging Organizations
The assets in our attack surface are frequently changing	61%	72%	60%	53%
We believe unknown or unprioritized assets are more susceptible to malicious attack	59%	79%	59%	52%

Expanding attack surfaces across the board has been a security challenge in recent years due to increased data collection, the proliferation of SaaS tools, and a move towards remote working. In 2020, the pandemic accelerated these trends considerably at a time when IT and security resources were already stretched. Innovation by hackers coincided with increasing demand for ASM solutions that go beyond passive scanning and asset inventory software, creating **a growing segment of the crowdsourced security market.**

Bugcrowd responded to this trend by launching a dedicated **ASM solution** at the end of 2019, the first of its kind to **leverage attack-minded defenders in support of scanners and automated tools.** This uses enriched skills profiles to find the hackers with the most applicable skills for the job and works with these hackers to offer a finalized report that prioritizes assets by risk, along with recommended next steps.

The explosive growth we are seeing in ASM began with innovative hackers who implemented new and effective approaches to recon. Traditional recon took an "inside out" approach, starting with known assets and expanding outwards from those initial markers to discover more. We are now seeing growth in an **"outside in"** model where **researchers are scouring the entire internet in order to uncover relevant assets.** Hackers who were early movers in automation and identifying systemic risks, are the ones who tended to turn into million-dollar hackers. These hackers acted as R&D for the security industry as a whole and drove the uptake of services such as Recon.dev, BitDiscovery, and SecurityTrails.

Opening this Pandora's box showed an aspect of security that had previously received little commercial attention beyond some scanning tools, but represented a **rich vein of vulnerabilities for attackers.** Research showed a sector that best practice was also emerging within this security segment driven by internal collaboration between CISOs and CIOs as well as external work with the Crowd. Tight integration is at the heart of ASM, as we found that organizations with mature security find more vulnerabilities and invest more in managing their attack surfaces through crowdsourced security.

SPEED: THE HACKERS' COMPETITIVE ADVANTAGE

Standards of hunting have steadily increased as the sector matures, incentivizing innovation among hackers in the methods they use. Speed is becoming a competitive advantage for buyers looking to maintain security as well as for hunters looking to maximize their income. Some hunters have standardized their approaches and are sometimes even able to "spray" vulnerabilities across multiple programs.

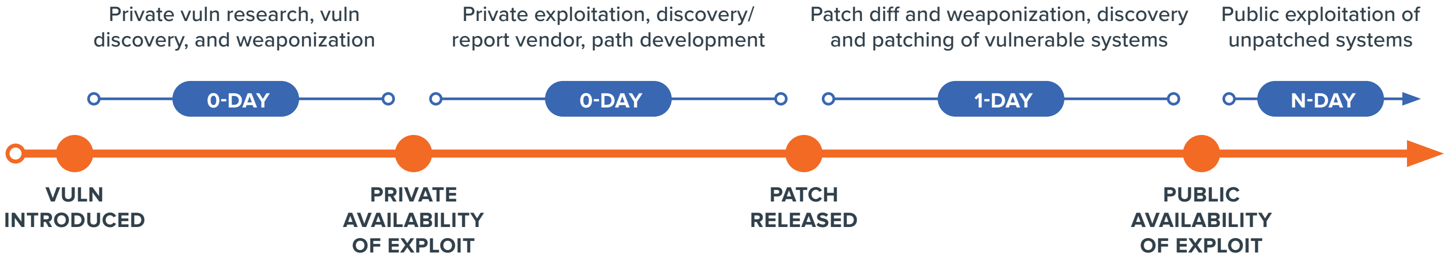
We see hackers identifying and applying exploits more quickly, sometimes even working in teams to deploy fresh exploits across bounty programs before their assets are patched. This speed is replicated by adversaries too, forcing security teams to take notice and **become more agile** in their response. Being able to quickly identify and remediate vulnerabilities is becoming a competitive advantage in today's globalized, connected world. Companies need a mix of security resources to **operate quickly and effectively,** causing crowdsourced security to move from "good to have" to "need to have."

EXPLOIT DEFINITIONS

0-DAY A software vulnerability that is being exploited but isn't known to the vendor. This means no fix is available.

1-DAY A software vulnerability which is known, and for which a patch is available to the general public. Typically 1-days are exploited by reverse-engineering exploits from vendor patches.

N-DAY A vulnerability that has had a patch freely available for some time. Systems that do not regularly update their software are vulnerable to N-days.

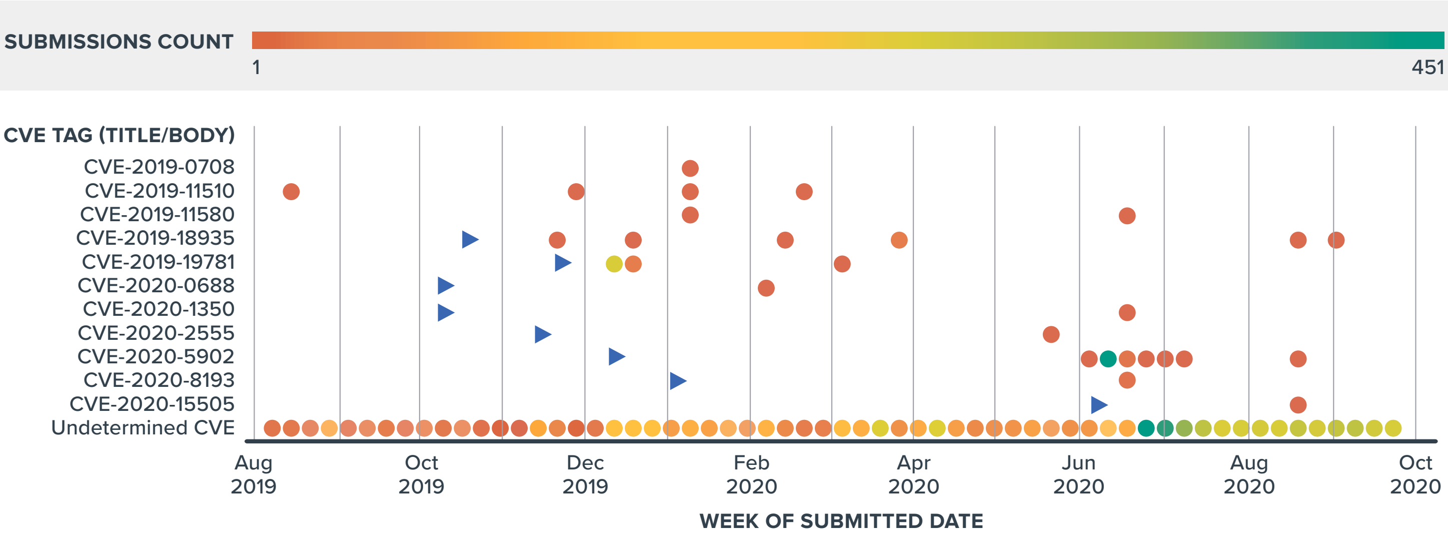

Private vuln research, vuln discovery, and weaponization
0-DAY
Private exploitation, discovery/ report vendor, path development
0-DAY
Patch diff and weaponization, discovery and patching of vulnerable systems
1-DAY
Public exploitation of unpatched systems
N-DAY
VULN INTRODUCED
PRIVATE AVAILABILITY OF EXPLOIT
PATCH RELEASED
PUBLIC AVAILABILITY OF EXPLOIT

When vulnerabilities are first discovered, they can sometimes be sold to offensive brokers and weaponized as 0-days before being traded to nation states for offensive use. Vendors will often become aware of vulnerabilities through crowdsourced security channels such as VDPs or bug bounty programs, allowing them to build a patch. This in turn allows enterprising hunters to reverse-engineer a 1-day from the patch and systematically deploy it in other bug bounty programs. Patches should eventually be widely available, but the vulnerability could live on and continue to create risk as an n-day.

Zero-day exploits continue to grab headlines, supporting a widespread belief that nation state actors and Advanced Persistent Threats are wielding an array of advanced attacking weapons that defenders are powerless to stop. This is harmful, as it breeds learned helplessness that reduces security standards. Advanced cyber adversaries are successful by basing the majority of their work on known exploits, as the NSA demonstrated when it recently released an advisory on Chinese cyber activity that showed their tactics were based mostly on n-days. Dealing with these exploits quickly and efficiently is a **considerable source of competitive advantage** even against the world's most skilled adversaries.

Bugcrowd data shows that our hunters were uncovering these vulnerabilities as they were deployed by the APT, acting as an important line of defense that ultimately overlaps with national security. Even against the most skilled actors, **crowdsourced security represents a formidable layer of defense.**

CROWD SUBMISSIONS OF CHINESE CVEs



POLICY CHANGES:

THE DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA

The Digital Millennium Copyright Act (DMCA) makes it illegal to circumvent controls on access to copyright material, amended in 2016 to allow for good faith security research.

THE COMPUTER FRAUD AND ABUSE ACT (CFAA)

The Computer Fraud and Abuse Act (CFAA) prohibits access to a computer without authorization. The Department of Justice acknowledged that it **remains an issue** for consideration when conducting security research.

UNITED STATES V. VAN BUREN

United States v. Van Buren, a case before the Supreme Court that addresses the scope of the CFAA with potential repercussions for good faith hackers.

VOATZ AMICUS BRIEF

Voatz amicus brief a submission to the Supreme Court by a voting tech company calling for an expanded interpretation of the CFAA.

DISCLOSE.IO

Disclose.io a cross-industry nonprofit committed to standardizing best practice in vulnerability reporting and research. Filed **a response to the Voatz amicus brief** with widespread industry support.

NIST SP (800-53)

NIST SP (800–53) guidelines from the National Institute of Standards and Technology (NIST) adopted at government level and revised for the fifth time in September.

BINDING OPERATIONAL DIRECTIVE 20-01

Binding Operational Directive 20-01 a directive issued by the Cybersecurity and Infrastructure Security Agency that calls for all federal civilian agencies to set up VDPs within six months.

Hacking has been a feature in law and public policy ever since **the movie WarGames** inspired Ronald Reagan to address cyber warfare through policy and legislation. Both the DMCA and the CFAA were drafted when hacking was considered to be a purely malicious activity, which we covered in detail in our **Ultimate Guide to Vulnerability Disclosure**. The law around hacking will soon be clarified, when the Supreme Court considers whether improper use of software can amount to criminal conduct in cases where the user is authorized, but the specific use is not.

HOW YOU CAN MAKE A DIFFERENCE

An expansion of the CFAA would be a **disaster for security research.** Hackers authorized to test software could be found guilty of breaking the law due to accidental overreach or poorly outlined scope. It is like threatening prison time for jaywalkers in a city where pedestrian crossing signs are ambiguous looking and difficult to identify.

Private companies and nonprofit groups have been making their voices heard on the issue, as this area of law is less mature than the industry it regulates and judges will not have much technical knowledge of the relevant cases. White hat hackers are an **essential resource to improve cyber resilience for governments and private companies** across the world. Bugcrowd is encouraging hackers and security professionals at all levels to support ethical security research. In-house professionals can do this by updating their status on disclose.io and considering expanding their scope. Hackers should endeavour to be tenacious but empathetic when reporting vulnerabilities. The hacking community is incredibly diverse, but kindness is a universal virtue we can all commit to.

Another recent development is NIST's fifth revision to update to **SP (800–53) Guidelines**, which represents a significant step towards acknowledging and encouraging the contribution of hackers to mainstream security controls. This **recommends organizations include bug bounty programs**, which helps bring crowdsourced security further into the mainstream and expand the market. But it is in the area of vulnerability disclosure that the recommendations make a truly progressive case.

The update calls for organizations to **adopt VDPs as standard**, positioning them as a superset base that can be built upon with layers such as bounty programs or pen tests. This even advises organizations to provide hackers with credit for their work discovering vulnerabilities by advocating for timeline-driven, coordinated vulnerability disclosure, the most hacker-friendly approach to disclosure. This is topped off by an explicit recognition that "organizations generally expect that such research is happening with or without their authorization," positioning public disclosure channels as **an opportunity to benefit** rather than suffer from ongoing hacking.

Broad adoption of SP 800-53 at government level has made it a de facto standard for much of the corporate world in the USA and globally. It builds on the binding operational directive from the Cybersecurity and Infrastructure Security Agency that calls for all federal civilian agencies to set up VDPs within six months. Because the US is the world's largest digital economy, it often acts as a bellwether for security norms and regulation, meaning these decisions will **help accelerate the move towards normalizing hacking**, fair disclosure, and crowdsourced security as central parts of mainstream security.

We know from experience that progress in security involves steps backwards as well as forwards, but the last year has been a positive one for security policy overall. As ethical hacking continues to grow, **recognition and awareness of crowdsourced security is improving.** And while we still encounter some regressive knee-jerk reactions, the vast majority of those in the US government and wider security industry see the benefits of the sector. We expect this to continue and the leadership shown within the US to expand to international governments.

NON-BUG USE CASES

Mainstream adoption of crowdsourced security led the offering to develop and mature, expanding from humble origins testing web applications to **more advanced implementations.** Bug bounties are showcasing the ingenuity and ability of the Crowd to solve security problems, leading companies to engage hackers for source code analysis, privacy bounties, and similar abstract security tasks. This brings the Crowd deeper into the SDLC and further legitimizes **crowdsourced security as a crucial element in the security stack.**

Facebook is an example of a company that has been backing its **strategic push for privacy** with hard cash, introducing **data abuse bounties** for passively identified privacy bugs in third party apps in 2018. This was followed by **Google introducing similar bounties** covering the Play Store, Chrome, and anything with access to the Google API. Facebook **expanded this to active testing** in late 2019, although this requires permission from the associated third party. Privacy bounties allow hackers to bridge the gap between policies and operations, finding "abuse cases" that bring together law, policy, and code. Investing in these rewards is an effective way to reduce risk from privacy regulation such as the European Union's **GDPR** or California's **CCPA**. It is also possible that the tech giants are ramping up these efforts to improve their reputations at a time when calls for antitrust action in the US are growing louder.

Hackers are also going right to the core of SDLC testing with assignments at every level of the security stack. These engagements are becoming more akin to white box testing, where researchers have full access to the application's source code. Here the US government is again leading the way, with **the Air Force commissioning Bugcrowd** for an assignment that included social engineering, internal network testing, and source code analysis.

Bringing the Crowd closer to sensitive assets requires **high levels of trust and security clearance**, especially for government clients. This requires hackers to provide more detailed identification within the Crowd, and this trend is in turn driving hackers to build more of an individual brand and profile for their work. While the anti-establishment culture is still alive and well within the hacking community, the professionalization of the industry allows the market to expand into sectors such as government and defense that have higher standards of compliance.

The broadening scope of crowdsourced security assignments led many within the industry to reconsider hacking and security research on a conceptual level. **What began as a synonym for software testing is now becoming a mindset, outlook, and way of engaging with the world.** Hackers without legal training are able to see policy as code, stretching and applying it until cracks and gaps emerge. Governments and corporations are using the Crowd as a flexible resource rather than a party in a transaction, broadening the scope of their assignments to use hackers to test business and legal logic as well as technical problems. This suggests there will be **continued growth and success for crowdsourced security.**

> While the anti-establishment culture is still alive and well within the hacking community, the professionalization of the industry allows the market to expand into sectors such as government and defense that have higher standards of compliance.

GETTING STARTED WITH CROWDSOURCED SECURITY

In 2020, we learned that corporate security needs are broad and can change rapidly in response to changes in the threat landscape. Security tasks demanded by the market are becoming more niche, from privacy bounties and source code analysis to hardware hacking and ASM. Mature organizations accept that it is not economically viable to hire all necessary talent in-house and are turning to the Crowd, creating competition within the industry regarding how best to service these new and wide-ranging demands.
At Bugcrowd, we built the Crowdmatch engine to offer automated staffing for programs by **matching the right cybersecurity talent to a customer's cybersecurity tasks.** Crowdmatch moves away from a static relational database of researchers to a more efficient categorization of researchers that creates a customer "context" prior to matching, making the process more streamlined and efficient. This ensures customers can **quickly get access to the correct skills and resources no matter how specific and niche their requirements.**

The scale and complexity of contemporary security challenges brings crowdsourced security into the industry mainstream, and we predict it will only grow in importance. Different applications of the Crowd are suitable based on a buyer's security needs and overall maturity, and it is worth considering how each can be used.

Companies looking to add crowdsourced security to their security mix should start by checking out **Bug Bounty Programs.** These tap into the Crowd to give buyers access to trusted white hat hackers who will continuously hunt for vulnerabilities across a variety of designated attack surfaces. By partnering with Bugcrowd, you **only pay for results and don't have to worry about reporting triage, relationship management, or vetting.**

Buyers also need to maximize their use of crowdsourced security by ensuring their programs are correctly incentivizing hackers to contribute their time and expertise. Bugcrowd research shows that the number of critical vulnerabilities found in the first 90 days of a program correlates to the size of the reward offered for P1 and P2 vulnerabilities. This is a benefit to security teams, as it allows them to budget effectively by paying for results and knowing their investment is being used efficiently.

While triaged and prioritized bounty programs will deal with the most urgent concerns, it is also important to **maintain a dialogue with the security community** regarding all assets. Because a company's assets change on a daily basis, the way to stay on top of potential vulnerabilities is to institute a **Vulnerability Disclosure Program (VDP).** These provide a framework for receiving and acknowledging vulnerabilities found by researchers, and Bugcrowd's service here again handles triage and communication. For more please see our **Ultimate Guide to Vulnerability Disclosure**.

Many companies need more structure in their security testing, either to prioritize certain assets or to meet compliance standards. Here a crowdsourced security pen test is most appropriate, and this could be **Classic or Next-Gen.** This offers continuous or on-demand service in a more efficient and cost-effective model than industry incumbents.

Finally, as a company's assets and data footprint grow, it creates indeterminate risk around forgotten and unknown assets. Here hackers can be deployed as recon using an **ASM program.** These offer results better than what is available from scanning tools by leveraging hackers' insight and awareness to identify, assess and prioritize vulnerabilities related to Shadow IT. Research with ESG shows that **the most mature organizations invest in ASM as a way to stay on top of emerging risk** by using continuous scanning and live alerting when vulnerabilities emerge.

A BUGCROWD OVERVIEW

PUBLIC AND PRIVATE BUG BOUNTY

Bug Bounty programs enable organizations to incentivize trusted white hat hackers to continuously hunt for vulnerabilities across a variety of designated attack surfaces. Bugcrowd's fully managed approach includes researcher matching, vulnerability prioritization, and program health monitoring.

Top Talent: Access to thousands of uniquely skilled, trusted motivated and incentivized Researchers.

Rapid Risk Reduction: An incentive-based approach motivates Researchers to find high-impact vulnerabilities.

Cost-Effective: A results-driven model ensures you pay for vulnerabilities that present a risk, and not the time or effort it took to find them.

VULNERABILITY DISCLOSURE PROGRAMS

Bugcrowd VDP provides a coordinated channel and framework to enable anyone, anywhere, to responsibly disclose security vulnerabilities found in publicly accessible assets. Bugcrowd's fully managed approach reduces noise and accelerates remediation.

Demonstrate Security Maturity: Build stakeholder confidence and trust by protecting digital assets and responding to known risks.

Formalize Security Feedback: Create a channel for security feedback and a framework to manage discovered vulnerabilities.

Meet Compliance Requirements: Align cybersecurity programs with best practices, as defined by the US Government, NIST, DOJ, FDA, and others.

CLASSIC AND NEXT GEN PEN TEST

Bugcrowd's Pen test portfolio infuses the platform-powered Crowd intelligence into both pay-per-project and pay-per-finding penetration testing. Testers follow a set methodology with QSAC-assessed final reporting to help meet compliance objectives.

Continuous Coverage: Choose between on-demand or continuous testing styles, with options for vulnerability-based incentivization to increase coverage and reduce risk.

Faster Launch: Ditch scheduling delays with access to more skilled and available testers. Most programs launch in as little as 72 hours.

Day 1 Vuln View: Don't wait until final report delivery to see what's wrong. Bugcrowd's platform provides visibility into vulnerabilities the second they are submitted.

ATTACK SURFACE MANAGEMENT

Bugcrowd's Attack Surface Management portfolio helps organizations reduce risk from unknown, or unprioritized assets that often become a primary target for attackers. Asset recon experts hunt for unseen assets, while a software-based solution continually scans for new connections and activity.

Reduce Unknown Attack Surface: Find forgotten assets that scanners can't. Receive priority risk-ranking based on each asset's potential for vulnerability.

Continuous Scanning: Asset Inventory leverages a pre-indexed snapshot of the internet which continues to grow. New assets are added to your inventory as they are discovered and attributed.

Live Alerting: Receive alerts on high-risk events like open ports or soon-to-be-expired security certificates. Share findings with external teams like marketing, sales, and product to ensure quick fixes.