

THE RISE OF THE BIONIC HACKER

HACKER-POWERED SECURITY REPORT

> 9TH EDITION

| hackerone

Table of Contents

Part I	
AI's Transformative Impact on Cybersecurity	3
Part II	
The Human Advantage in Cybersecurity	9
Part III	
Building Best-in-Class Security Programs	14
Industry Insights 2025:	
Bounties, Breaches, and Business Risk	20
Closing Remarks	28
Data Sources and Methodology	29

Executive Summary

Since 2024, HackerOne has seen a 210% increase in valid AI-related vulnerability reports and doubled the number of surveyed researchers focused on AI/ML assets.

From automakers to government agencies and global banks, today's enterprises are fundamentally technology-driven and operating in threat landscapes that evolve faster than ever. Accelerated by the mainstream adoption of AI and the erosion of traditional perimeters, modern attackers combine automation with creativity to exploit vulnerabilities at machine speed, often before defenders even recognize the threat.

We're witnessing the emergence of a new kind of security contributor:

THE BIONIC HACKER

These are human security researchers using AI as a catalyst, accelerating recon, triage, scaling pattern recognition, and probing complex attack surfaces faster than ever before. The gap between traditional automation and human testing is closing; not because humans are being replaced, but because they are evolving with AI.

In our 9th annual Hacker-Powered Security Report, we reveal how AI is reshaping offensive security into a more continuous and contextual process, and why the future belongs to teams who treat AI not as an add-on, but as a core extension of human expertise.

Drawing from extensive data gathered from our global community of ethical hackers and security researchers, real-world experiences from customer engagements, and proprietary intelligence from the HackerOne Platform, the 2025 report revolves around three pillars:



AI's Transformative Impact on Cybersecurity



The Human Advantage in Cybersecurity



Building Best-in-class Security Programs

About the Hacker-Powered Security Report

The 9th annual Hacker-Powered Security Report compiles insights, data, and analysis from customers, security researchers, and HackerOne's vulnerability database from July 1, 2024, to June 30, 2025.

580,000+

All Time Valid Vulnerabilities

1,950+

Customer Programs in 2025

99

Surveyed Customers

1,820+

Surveyed Researchers

Key Findings

Valid AI Vulnerability Reports Skyrocket in 2025

Out of the 210% increase in valid AI reports, **65%** were AI security issues such as prompt injection, model manipulation, or exposed endpoints, while **35%** fell into the AI safety category, including ethical misuse or output integrity. This surge is fueled by growing researcher interest: in 2024, just **9%** of survey respondents focused on hacking AI/ML assets. That number has now doubled to **19%**, signaling a strong shift in focus within the security research community.

AI Security Concerns Increase Among HackerOne Customers

In 2025, **78%** of HackerOne customers said their concern over AI risks had grown in the past year. Just a year earlier, less than half (48%) ranked generative AI among their top security risks.

The shift shows how quickly AI has moved from a watch list item to a front-line security concern, especially around data integrity and misuse.

HackerOne Researchers Are Preparing for the AI Era

58% of surveyed security researchers are actively upskilling in AI, learning to audit AI/ML systems, and integrating AI into their own workflows.

The rise of bionic hackers, humans pairing their creativity with the scale and speed of autonomous and agentic tools, is already shaping the next generation of offensive (and defensive) security capabilities.

Year in Review

\$81M

^{^ Up 13%}

Total Bounty Payouts

\$1,090

^{^ Up 4%}

Average Bounty Payout

84.9K

^{^ Up 7%}

Valid Reports

23.7K

^{^ Up 10%}

Critical & High Severity Valid Reports

1,121

^{^ Up 270%}

Programs with AI in Scope or with a Valid AI Report

210%

^{^ Up}

Growth in Valid AI Reports

339%

^{^ Up}

Rewards Paid Out for Valid AI Reports

\$3B

^{^ Up 9%}

Mitigated Loss Savings

Part I - AI's Transformative Impact on Cybersecurity

In 2025, 13% of organizations reported an AI-related security incident. Of those, 97% lacked proper AI access controls.

As organizations race to deploy AI, many still lack the capacity to secure it.

According to IBM's Cost of a Data Breach Report 2025, 97% of reported AI-related security incidents had gaps in access controls.

Our customer survey echoes this: more than half feel unprepared and under-resourced for AI risks. While [84% of CISOs](#) now oversee AI security and data privacy, many report they lack the resources to manage these risks effectively.

Since our last report, AI has expanded from isolated models to a connected ecosystem.

New protocols and architectures now let systems operate with real-time context, coordinate across tools, and embed directly into security workflows. This shift is reshaping both sides of the HackerOne community: customers are rapidly bringing AI assets into scope, and researchers are growing the skills to test and secure them.

This first section follows that shift into practice through four lenses: securing AI itself, using AI to accelerate program operations, how researchers wield AI in their toolkit, and what hackbots add.

Security for AI

1,121

Distinct programs included AI in scope or received a valid AI vulnerability.

270%

Year-over-year increase of AI in program scope.

58%

Of the survey respondents have upskilled in AI/ML security.

41%

Of the respondents are already testing AI assets as part of their work.

A major enabler in 2025 was the [Model Context Protocol](#) (MCP), which provides LLMs structured, real-time connections to tools and data.

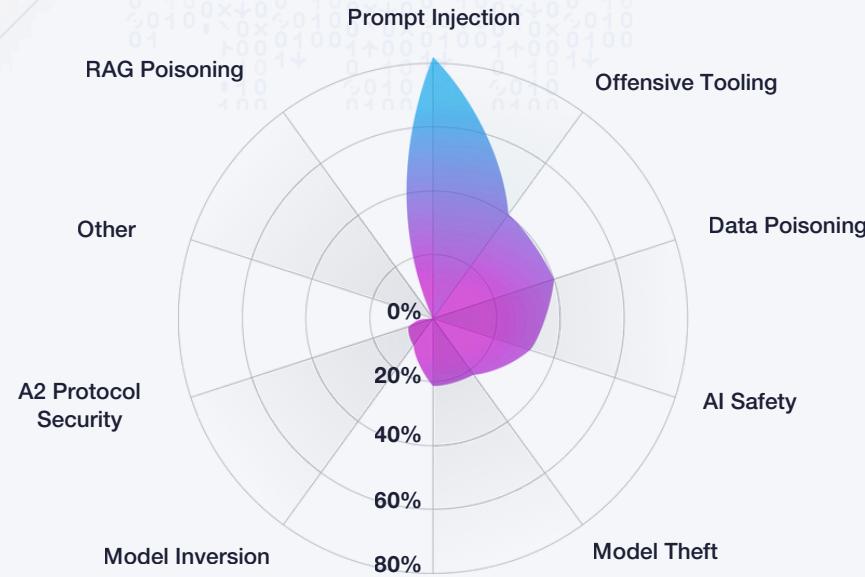
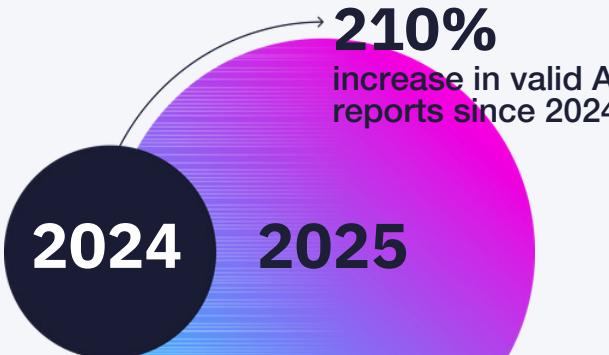


Figure 1 - AI/ML security skills of surveyed researchers

21% of surveyed HackerOne researchers (Figure 1) are developing MCP-specific security skills as these capabilities enter customer workflows, and an overwhelming 82% are developing skills specifically in Prompt Injection.

AI Attack Surface and Findings

As organizations integrate AI into products, workflows, and infrastructure, attackers are learning just as quickly how to exploit them.



339%
increase in total rewards paid
for valid AI vulnerabilities
from 2024 to 2025

Figure 2 - Growth of valid AI reports over time

Pillars of Trusted AI: Safety and Security

In 2025, 78% of customers reported growing anxiety over AI risks, reflecting the surge in vulnerability findings.

Prompt injection saw the sharpest increase in 2025, up 540% (Figure 3), as researchers targeted weaknesses in how models interpret and execute user input. Sensitive information disclosure more than doubled (+152%), highlighting the risk of AI unintentionally revealing private or proprietary data.

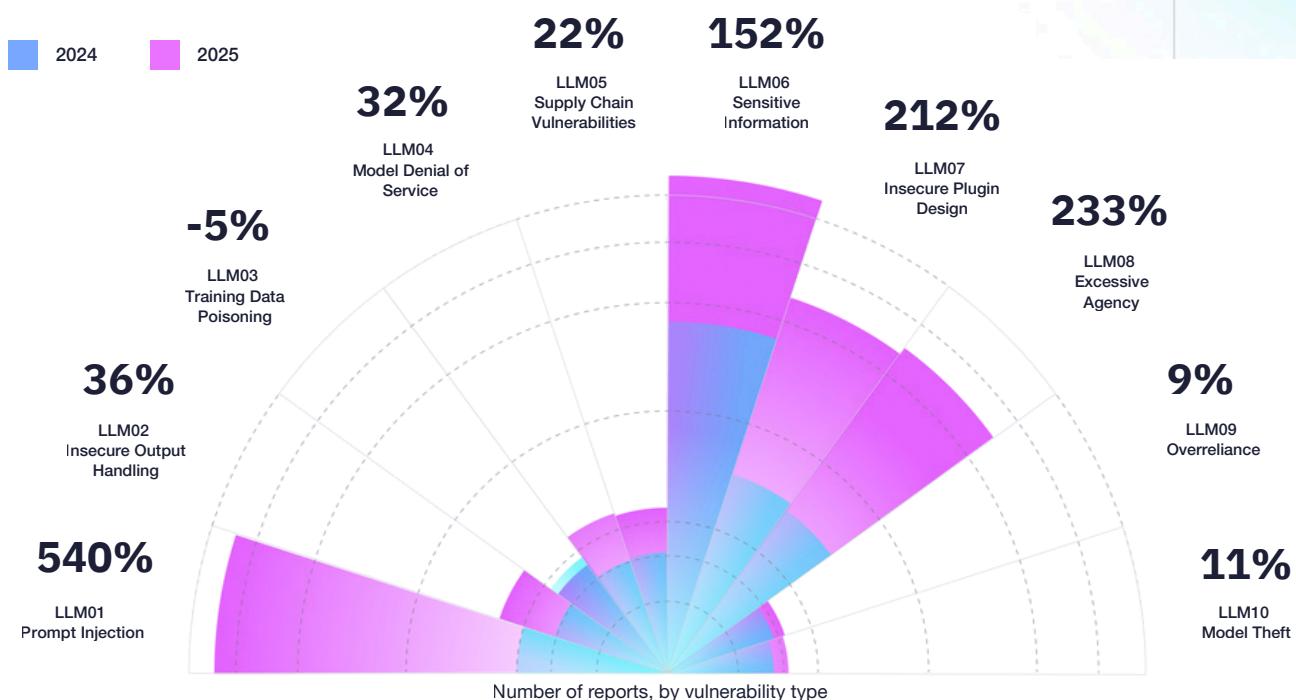


Figure 3 - Valid AI reports across OWASP Top 10, 2024 vs 2025

AI for Security and Program Operations

Since 2021, valid vulnerability reports on HackerOne have grown by **20%**, not including the large number of submissions ultimately deemed invalid.

Every report, whether critical or false, demands triage, creating a workload that quickly becomes unsustainable. Manual processes alone can't keep pace with the speed and scale of modern threat exposure management.

Hai, HackerOne's Agentic AI System

In 2025, 90% of HackerOne customers have enabled Hai, our agentic AI system. More than just an automation tool, Hai delivers AI for security outcomes and is redefining threat exposure management.

3 in 5

customers cite time savings and efficiency as Hai's biggest impact.

60%

save ~2 hours per week (~4-8 hours per month, about half to one full day saved).

20%

save 6–10 hours per week (~24–40 hours per month, equal to 3 to 5 workdays saved).

How Has Hai Impacted Your Workflow?



Figure 4 - Customers' workflow improvements by Hai

How Much Total Time Does Hai Save Your Team per Week?

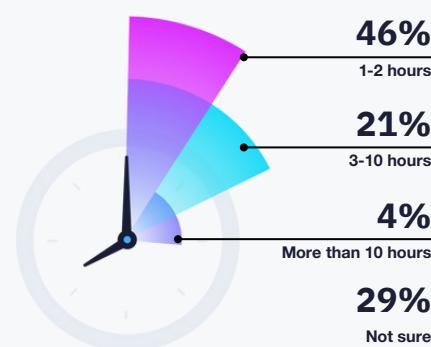


Figure 5 - Customers' time savings with Hai

AI in the Researcher Workflow

Just as customers are embedding AI to manage rising report volumes and improve program efficiency, researchers are rapidly embracing AI to sharpen their edge. 67% of surveyed researchers now use AI or automation tools to accelerate reconnaissance, speed up testing, and reduce repetitive tasks.

How Are You Using AI in Hacking?

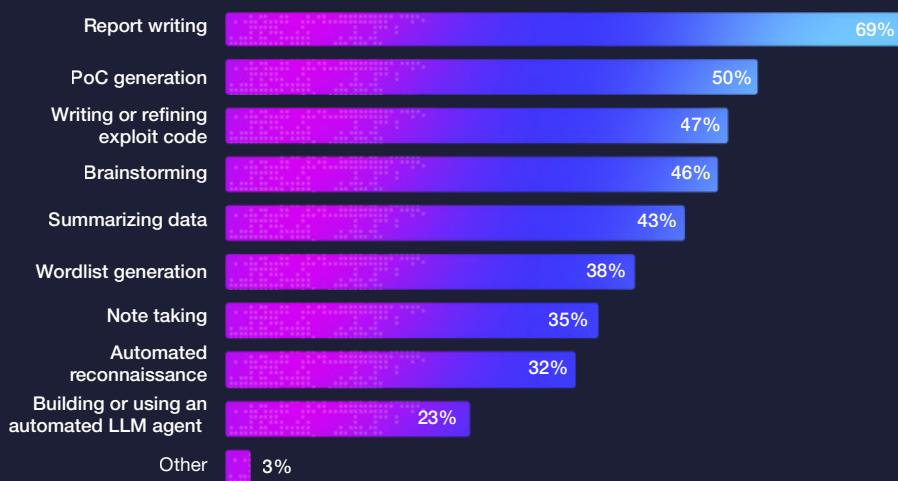


Figure 6 - The use of AI in hacking

Tools of Choice

Researchers are experimenting broadly, combining web-based LLMs, locally hosted models, and custom-built offensive tools to fit their workflows.

Web-based LLMs are valued for their accessibility and versatility (Figure 7).

Locally hosted models are gaining ground, among the 18% of researchers who cite privacy concerns as a barrier to cloud-based tools (Figure 8). These models provide power and control for sensitive or proprietary testing.

While privacy is a valid concern, the biggest blockers researchers face in adopting AI are 'Limited access to AI-specific training or resources' (39%) and a 'Lack of practical experience or expertise in AI security' (33%).

Web-based LLMs: What AI tools are you using?

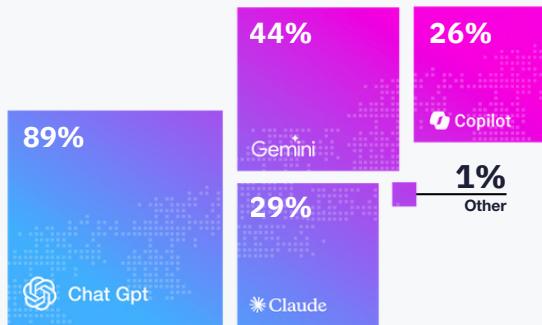


Figure 7 - Web-based LLMs used for hacking

Locally Hosted LLMs: What AI tools are you using?

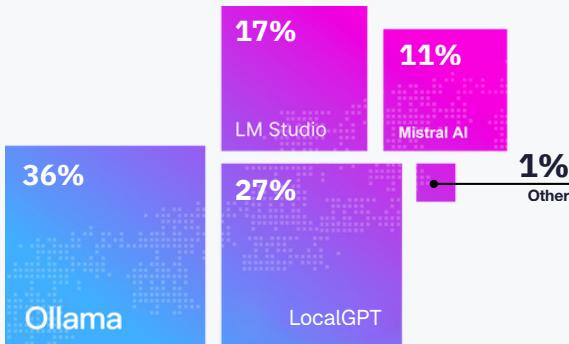


Figure 8 - Locally hosted LLMs used for hacking

AI-Enhanced Tools Leading Early Adoption

Burp AI (36%)



integrates AI directly into Burp Suite for attack analysis, with its usage growing at ~25% month over month.

Cursor (26%)



is used for AI-powered coding and debugging environment, alongside custom CLI wrappers (23%).

BurpGPT (20%)



is bringing natural language and automation into everyday workflows.

“

[At PortSwigger], our vision for Burp AI has always been simple: to augment researchers, not replace them. The significant levels of adoption we're seeing show that the community values AI that strengthens their skills. Burp AI is only the beginning. We're iterating fast and can't wait to see how it continues to evolve.”

— Katie Warren, Product Manager for Burp AI, PortSwigger

From Automation to Autonomy: The Hackbot Arms Race

With the rise of [agent frameworks and hackbots](#) in 2025, offensive security has entered the era of agentic AI. Unlike traditional scanners, hackbots and autonomous agents can already chain tools together, adapt to feedback, and make decisions in real time. This marks the move from rule-based automation to exploratory, AI-assisted offensive action.

Our [5-month review](#) tells us that hackbots excel at pattern-matching and detecting surface-level flaws like reflected XSS, much like traditional scanners.

As the technology matures, its capabilities will likely expand to uncovering IDORs or business logic issues at scale, but today, human contextual reasoning, and system-level understanding remain essential alongside automation and autonomy.

“

“The future is a symbiosis between hackers and AI. Hackbots can replace the repetitive work so humans can focus on creativity and new research.”

– André Baptista, long-time hacker, co-founder of Ethiack

”

Hackbots on HackerOne

6

560+

Unique hackbots submitted reports

78%

Valid submissions were XSS vulnerabilities

49%

of all hackbot reports were valid

HackerOne has already adapted, updating [its leaderboard](#) to represent all contributors, from individual researchers to collectives; highlighting a future where human creativity and AI's scaling power work hand in hand.

82%

of customers are aware of hackbots operating on the platform, **63%** remain cautiously optimistic, recognizing the opportunities and the risks they bring.

66%

of researchers expect hackbots will enhance their work, while **43%** see them mainly as tools for simple bugs.

How do you anticipate hackbots and autonomous testing tools will be used in the next three years?

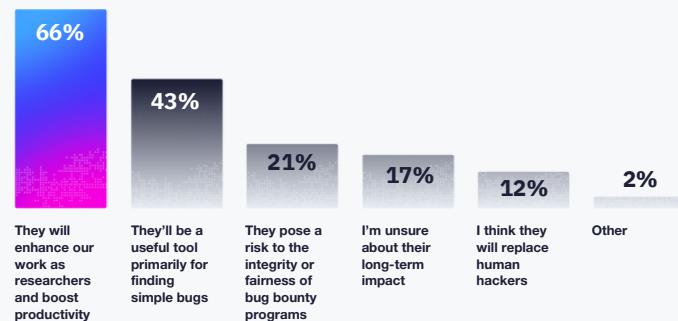


Figure 9 - The future of hackbots and autonomous testing tools



Part II - The Human Advantage in Cybersecurity

Only 12% of researchers believe AI will replace them. Most see the future of cybersecurity as a collaboration.

AI delivers speed, scale, and pattern recognition, while humans bring the nuance, creativity, and judgment needed for complex vulnerabilities.

Certain challenges, such as business logic flaws, multi-step exploits, and authentication bypasses (Figure 10), still demand human context and system-level understanding. When paired with AI's strengths in reconnaissance, scanning, and payload generation, researchers are able to identify risks more effectively.

Which Vulnerabilities are AI Tools Currently Weakest at Identifying?

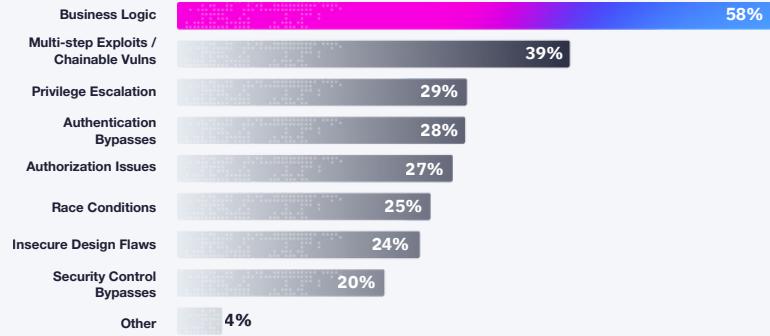


Figure 10 - The limitations of AI tools

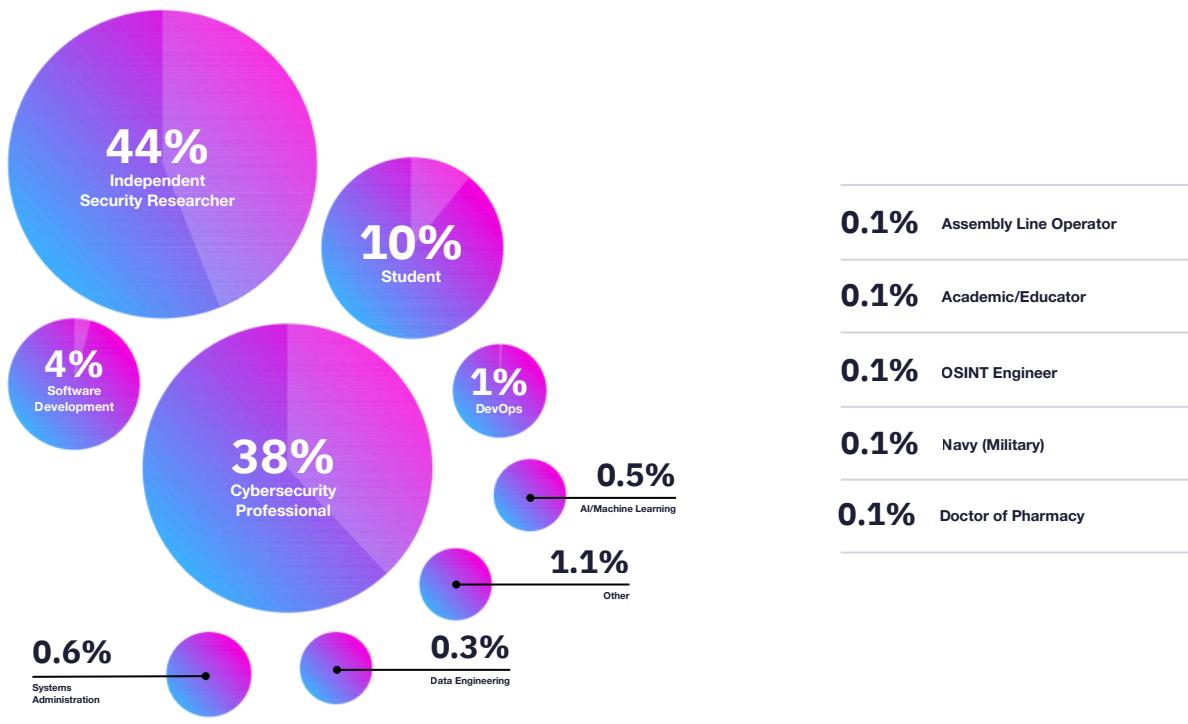
Building on this dynamic, this section explores how humans and AI complement one another in security, then turns to the HackerOne community itself; a global workforce that mirrors adversaries in creativity, but channels those skills toward defense.

Global Researchers, Diverse Impact

Security leaders often frame the talent shortage in terms of their own headcount, a view reinforced by ISC₂, which estimates global demand for 10.2 million professionals against a workforce of just 5.5 million, leaving a gap of 4.8 million. That gap reflects in-house staffing needs, but it overlooks the global researcher community: tens of thousands of skilled practitioners already finding and fixing vulnerabilities for enterprises every day.

This distributed talent pool is a force multiplier, bringing scale, diversity, and adaptability security teams cannot achieve alone. This year, we are bringing a sharper context on who these researchers are, where they come from, and how their expertise is evolving.

Multidisciplinary Backgrounds and Expertise

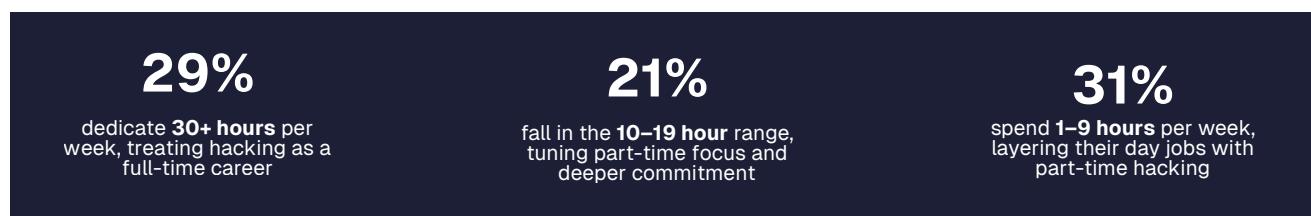


The HackerOne community is far from homogeneous (Figure 11). Nearly half of the survey respondents identify as independent security researchers, over a third as cybersecurity professionals, and 11% as students, with additional representation from DevOps, AI/ML, OSINT, and even unconventional paths such as pharmacy or assembly line operations.

This multidisciplinary mix is the secret recipe for producing technically sound, creative findings with the same persistence level as real adversaries.

A Flexible Workforce

Time commitment splits across a spectrum (Figure 12), creating unmatched flexibility among the surveyed researchers: a core of committed specialists, amplified by a broader perimeter of part-time experts who flex into programs as needed.



On average, approximately how many hours a week do you spend hacking (on another platform)?

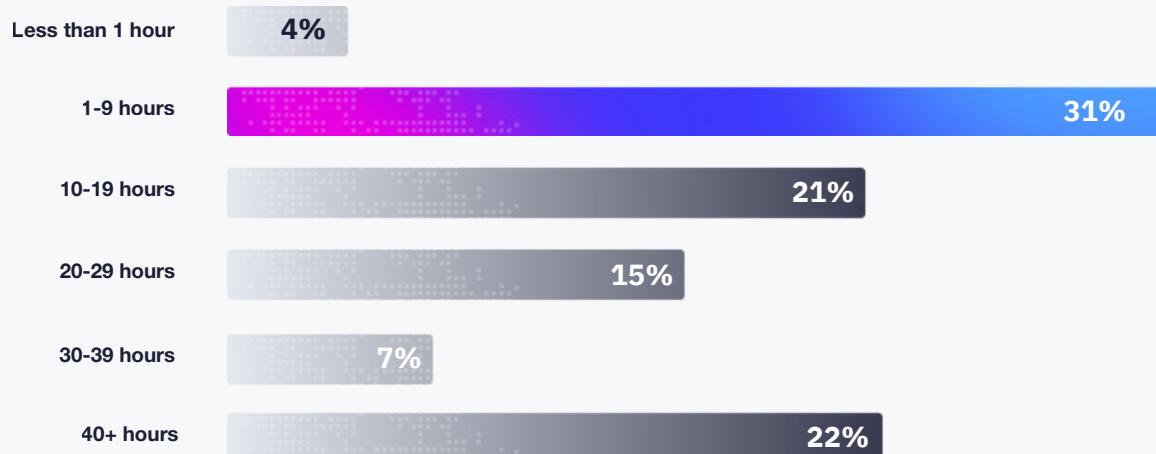
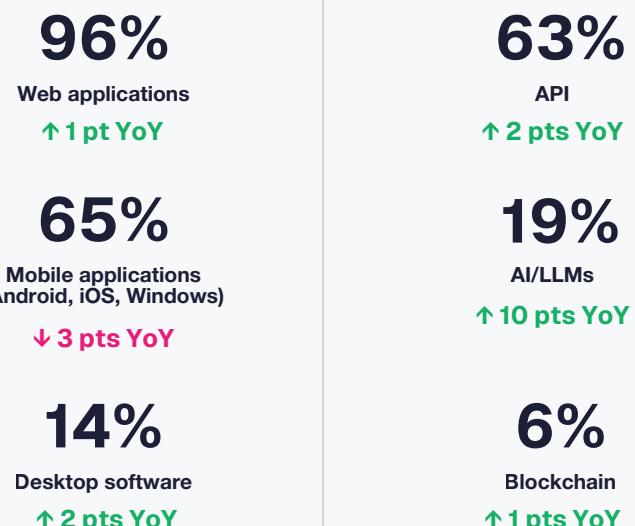


Figure 12 - Time commitment of surveyed researchers

Asset Focus

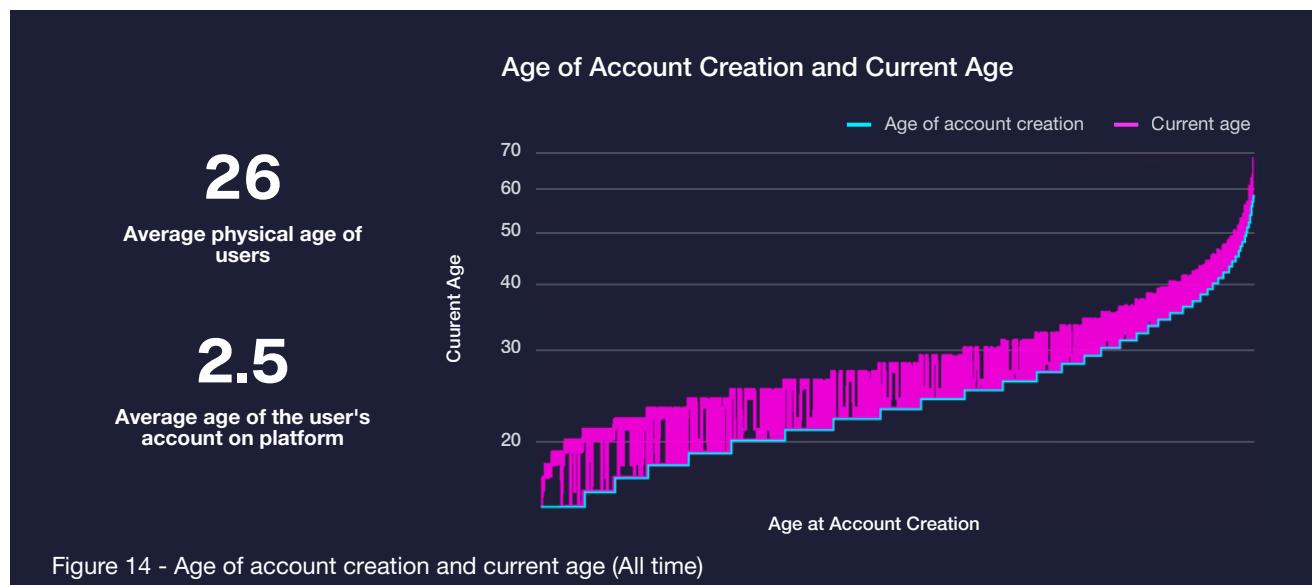
Researchers have the agility to shift quickly as new domains mature. The standout trend in 2025 is AI/LLM testing, which doubled YoY from 9% to 19% compared to figures in the [8th edition of the report](#).



Age and Maturity

Researchers often start young (late teens, early 20s), but our platform data shows a growing share in their 30s and 40s, even some in their 50s, signaling community maturity (Figure 14).

Payout data reinforces this (Figure 13): while many researchers contribute to the long tail, the most experienced capture six and seven-figure rewards, validating both their expertise and the market's demand for it.



24/7 Global Coverage

Geography underscores the adaptability of the HackerOne community, including security researchers, pentesters, and code reviewers. India, the United States, and the United Kingdom remain the largest hubs, but the community's footprint spans every continent. The percentages shown below are for the top 20 researcher home countries, representing 76% of the community; the remaining researchers are distributed across ~134 additional countries (Figure 15).

For enterprises, this global spread means always-on coverage across time zones and the benefit of regional perspectives that single-location teams cannot provide.

1	22%	India
2	15%	United States
3	4%	United Kingdom
4	4%	China
5	4%	Egypt
6	3%	Germany
7	2%	Turkey
8	2%	Indonesia
9	2%	Pakistan
10	2%	Brazil

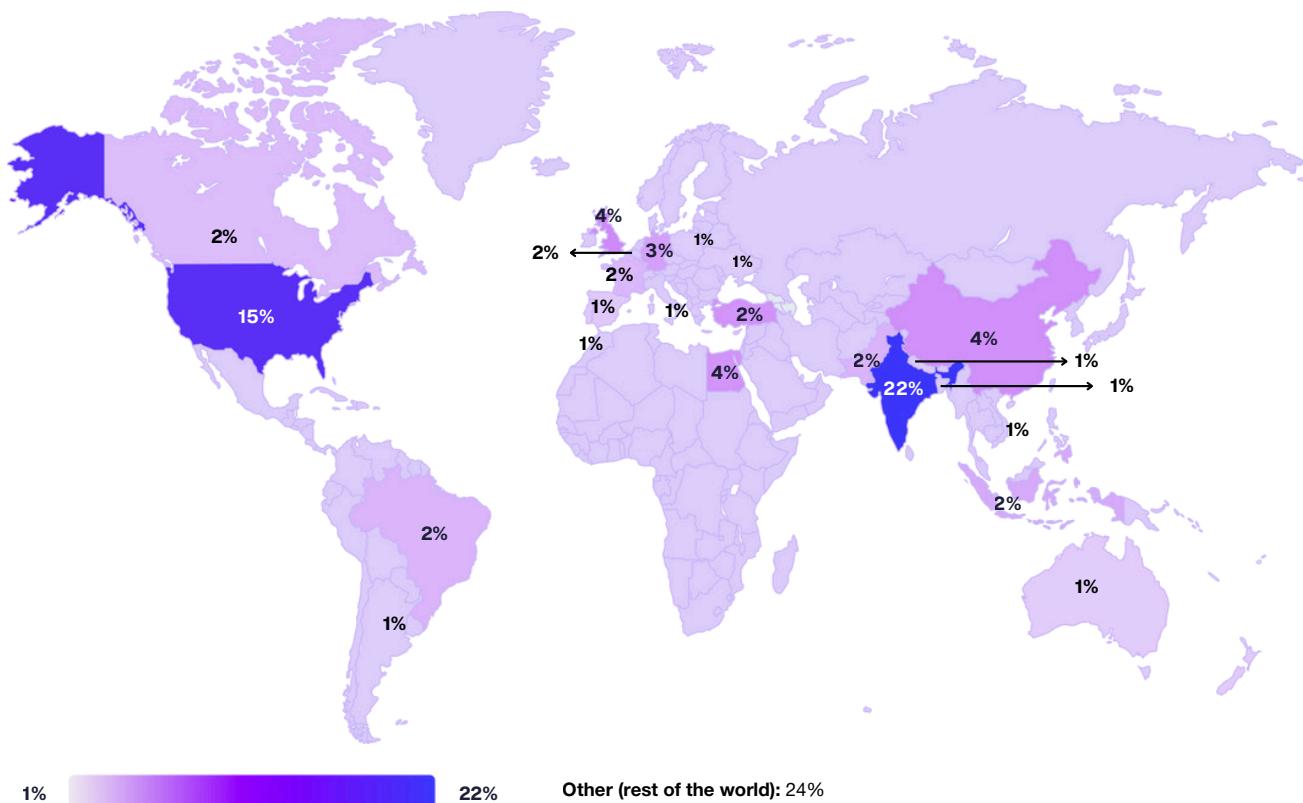


Figure 15 - Representation of HackerOne community members in top 20 countries (2025)

Part III - Building Best-in-Class Security Programs

65% of surveyed organizations report stronger outcomes after adopting a defense in depth approach, with bug bounty now in use at 83%.

Defense in depth highlights the value of layering safeguards and testing approaches to reduce the risk of a single point of failure. In the context of vulnerability discovery, combining methods such as code review, penetration testing, AI red teaming, vulnerability disclosure programs, and bug bounties ensures that different perspectives surface flaws that others may overlook.

However, layering defenses alone does not guarantee effectiveness. The true measure of success lies in how well findings are prioritized, how quickly the most exploitable risks are mitigated, and how seamlessly each layer of insight informs the next.

This section examines what makes security programs truly effective for organizations seeking resilience and for the researchers driving meaningful impact.

A Year in Review

In the past 12 months, HackerOne bug bounty programs collectively paid out \$81 million, an increase of 13% YoY. The top 10 programs alone accounted for \$21.6 million.

At the researcher level, the Top 100 all-time earners took a total of \$31.8M, with individual researchers now consistently surpassing six-figure annual earnings.

\$81M

Total paid out
in 2025

\$42K

Average yearly payout
across all active programs

\$7.6M

Total earned by top
10 researchers

\$31.8M

Total earned by top
100 researchers

\$21.6M

Total paid out by the
top 10 programs

\$51.4M

Paid out by the top
100 programs

Maturing Identity and Access: Signals from the Market

The YoY payout and valid report data (Figure 16) suggest positive signals in defenders improving identity and access security; however, the details matter.

Vulnerability Type	2025 Rewards (\$)	2025 Valid Reports
Cross-Site Scripting (XSS)	8,377,704 ↓ 7% YoY	13,197 ↓ 14% YoY
Improper Access Control (IAC)	8,797,644 ↑ 19% YoY	8,787 ↑ 18% YoY
Insecure Direct Object Reference (IDOR)	7,610,517 ↑ 23% YoY	6,016 ↑ 29% YoY
Information Disclosure	4,682,524 0% YoY	8,013 ↓ 2% YoY
Misconfiguration	2,717,656 ↑ 22% YoY	6,105 ↑ 29% YoY
Improper Authentication	2,353,009 ↓ 22% YoY	1,737 ↓ 9% YoY
Business Logic Errors	2,262,840 ↓ 5% YoY	2,001 ↑ 19% YoY
Code Injection	1,715,704 ↑ 10% YoY	1,043 ↓ 1% YoY
Server Side Request Forgery (SSRF)	1,521,303 0.5% YoY	822 0.2% YoY
Privilege Escalation	1,454,399 ↓ 7% YoY	1,766 ↓ 8% YoY
SQL Injection (SQLi)	1,302,696 ↓ 24% YoY	1,213 ↓ 23% YoY
Uncontrolled Resource Consumption	1,024,036 ↓ 11% YoY	659 ↓ 10% YoY
Improper Authorization	961,750 ↓ 43% YoY	1,168 ↓ 9% YoY

Figure 16 - Valid vulnerability reports and rewards comparison

Authorization taxonomies are changing labels

The drop in Improper Authorization, alongside the rise in Improper Access Control (IAC) and Insecure Direct Object Reference (IDOR), is proof that organizations have not solved authorization. Instead, it reflects a more precise classification of these vulnerabilities by researchers and triage teams.

While this improvement in taxonomy provides better clarity, the underlying risk of broken access boundaries across API's, microservices, and multi-tenant SaaS continues to climb.



Don't let shifting labels hide persistent systemic weaknesses.

Identity risk is improving

Improper Authentication fell in both payouts and valid reports this year, suggesting progress in hardening authentication flows and wider adoption of stronger identity providers.

Despite this decline, authentication flaws remain a high-value foothold for attackers, and prioritizing these vulnerabilities continues to be essential for business resilience.



The decline should be viewed as a sign of progress rather than closure. Continued investment in identity assurance and monitoring is essential.

Commodity bugs are entering saturation, accelerated by AI

XSS and SQL Injection are in decline, while Server-Side Request Forgery (SSRF) and Information Disclosure remain flat. This suggests that commodity bug classes are reaching a maturity point where they are no longer easy, high-value targets for attackers and researchers.

Hackbots are expected to accelerate this trend by increasingly automating the discovery and exploitation of these vulnerabilities, potentially reducing their relevance altogether.



Reallocate incentives, avoid overpaying for table stakes issues, while maintaining hygiene baselines to prevent attackers from exploiting residual long-tail risks.

Business logic flaws are the premium battleground

Valid reports for business logic flaws increased this year, highlighting the persistent difficulty in securing complex workflows and systemic abuse paths.

However, payouts for these vulnerabilities declined, suggesting programs are not consistently treating them as premium findings.



Business logic flaws remain high-risk. Align prioritization and rewards towards business impact.

Incentives Drive Outcomes

HackerOne examined 68 cases where programs reduced bounty payouts by at least 20% between 2018 and 2025. For each case, we measured valid vulnerability reports in the 12 weeks before the cut and compared them to the 12 weeks after. The pattern was consistent: lowering bounties led to fewer valid reports. Across all severities, programs averaged a 22% decline (Figure 17), while critical vulnerabilities dropped by half (Figure 18).

Impact of Critical Bounty Decreases (Weekly Analysis)

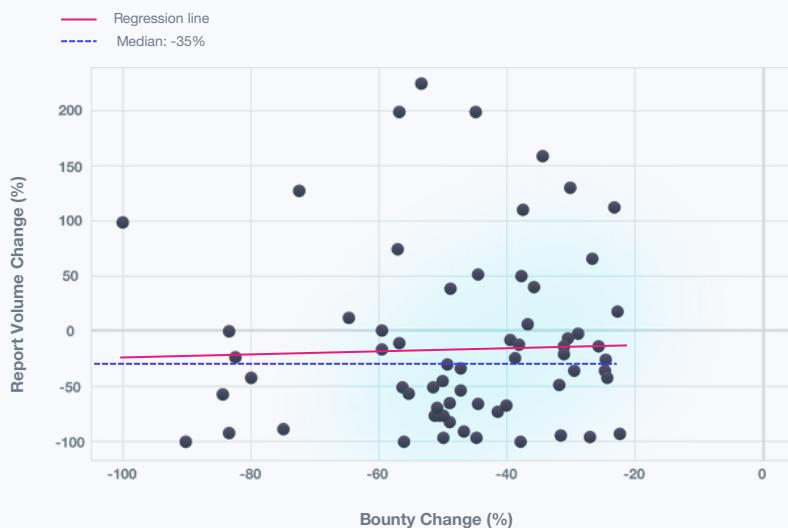


Figure 17 - Impact of total bounty decreases (weekly)

Impact of Critical Bounty Decreases (Weekly Analysis)

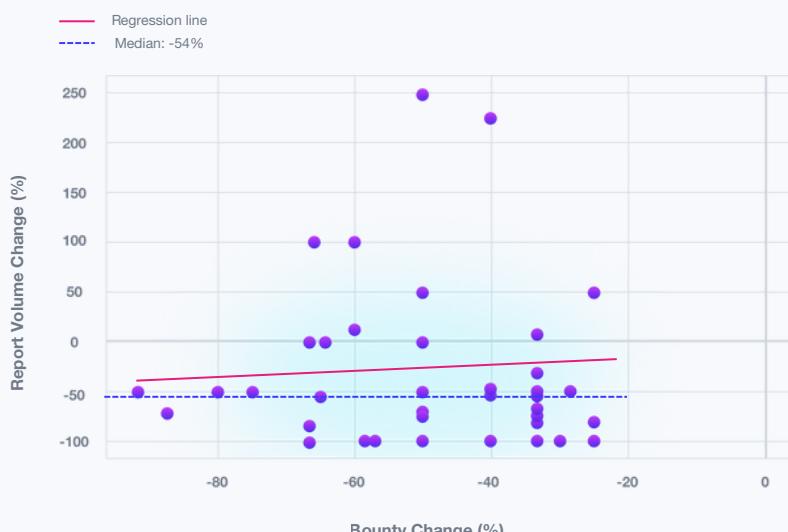


Figure 18 - Impact of critical bounty decreases (weekly)

73%

of programs saw a decline in valid submissions

22%

of programs saw an average drop in overall report volume

50%

of programs saw a decline in critical severity vulnerability submissions

Why it matters

Bounties are not cosmetic. When payouts fall, researchers disengage and the flow of valid reports slows. Maintaining competitive rewards is essential to sustain researcher participation and visibility into the highest-risk weaknesses.

The Five-Year Outlook: From Signals to Strategy

The YoY data (Figure 16) on page 15 highlights short-term shifts, but the five-year view (Figure 19) of the top 10 most common vulnerabilities confirms which signals are structural and which are noise.

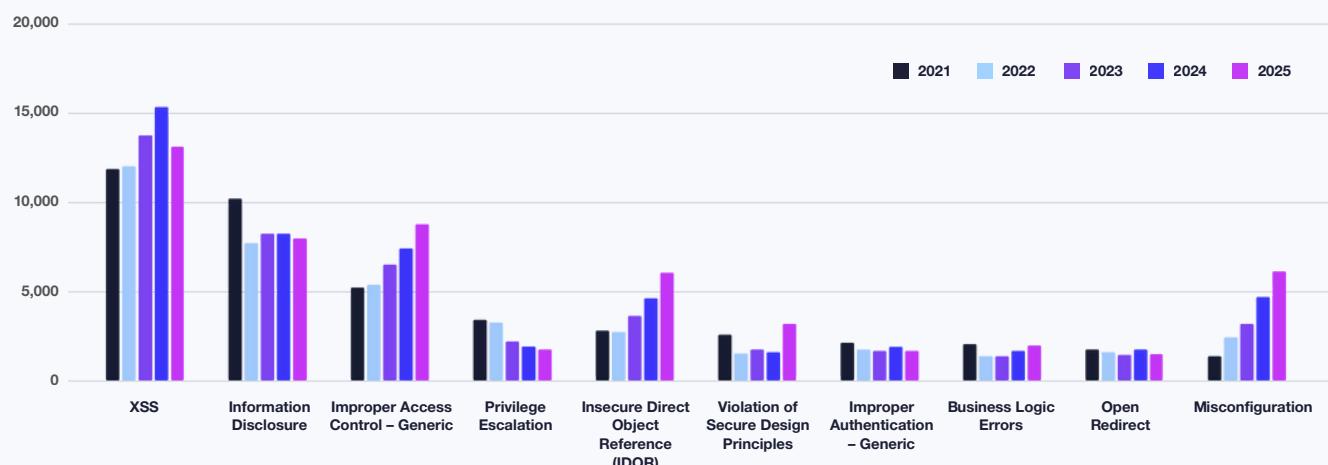


Figure 19 - Top 10 most common vulnerabilities YoY (2021-2025)

Authorization is structurally climbing

IDOR reports more than doubled in five years (+116%). Improper Access Control rose 66%. By contrast, XSS volumes grew only 10% in five years, with declining payouts.

The signal from one-year data is confirmed at scale: authorization is where attackers are concentrating.

Design-level flaws are rising, but undervalued

Violation of Secure Design Principles grew 21% over five years. Business Logic Errors climbed 19% in valid reports YoY, but payouts fell 5%.

Since 2022, these categories show steady growth in researcher attention without equivalent program investment.

Identity is steady in volume, steep in impact

Improper Authentication declined 20% in five years, echoing this year's short-term drop. Yet payouts remain disproportionately high relative to volume.

This confirms identity risk is not cyclical; fewer flaws are being found, but each carries a higher business impact.

Why this matters

Winning the next five years is about context and depth. Security leaders should use automation and emerging agentic workflows to keep commodity flaws like XSS and SQLi inexpensive, while prioritizing identity, access, and design-level weaknesses that drive material risk. The winning strategy is hybrid: agents and automation for scale, human ingenuity for impact.

Driving Program Effectiveness

Macro market signals set the direction, but program health is only secured in execution. Our 2025 survey highlights three fundamentals that define the healthiest programs (Figure 20).

What Program Behaviors Give You the Most Trust that Your Time Will Be Well Spent?



Figure 20 - Program behaviors that drive researcher trust

Scope clarity drives engagement: 85% of researchers view detailed scope documentation as the strongest indicator of program quality, and 72% prefer broader scopes.

Programs with fewer than five assets in scope consistently generated fewer valid submissions, underscoring the direct link between breadth and participation. Programs with scope updated in the last 6 months see over 4x more submissions compared to programs with updates older than 18 months.

Payout integrity builds trust:

Fair, consistent, and transparent payouts remain non-negotiable. Gaps between advertised and actual reward ranges continue to erode confidence when researchers feel misled or undervalued.

Triage speed sustains commitment: Average initial response times in hours improved by ~45% year-over-year (Figure 21), but pressure remains to professionalize workflows and deliver timely, constructive feedback that keeps researchers engaged.

Average First Response Time in Hours vs. Month

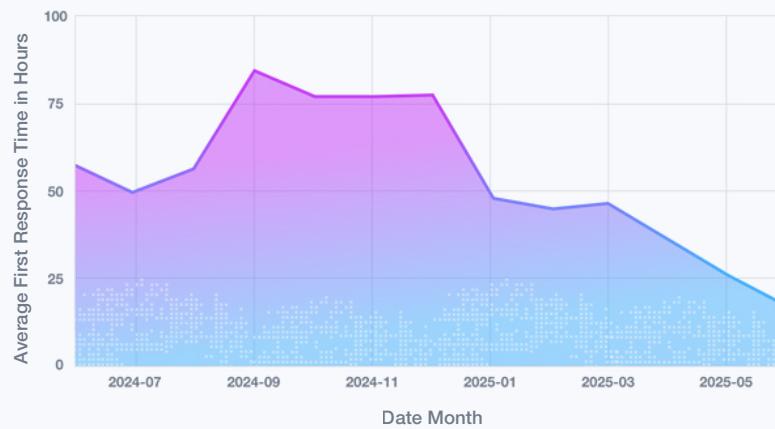


Figure 21 - Average first response time (in hours) vs months

Industry Insights 2025: Bounties, Breaches, and Business Risk

Verizon's 2025 Data Breach Investigations Report (DBIR) shows that vulnerability exploitation fell sharply this year, yet overall levels remain more than double those seen in 2022. A key accelerator of this risk is supply chain compromise.

SANS reports these incidents have surged more than 2,600% since 2018 and take the longest to detect and contain, 267 days on average. As organizations layer in AI tooling, pre-trained models, and third-party data pipelines, the surface area for compromise grows wider and harder to secure.

IBM Research sets the global average breach cost at \$4.44M, with U.S. organizations facing costs closer to \$9.45M.

We use breach cost benchmarks in our standard-setting Return on Mitigation (RoM) model to quantify avoided risk and losses. Applying this methodology across all HackerOne programs from July 1, 2024, to June 30, 2025, organizations realized \$3 billion in mitigated losses – equivalent to 15x returns, meaning for every dollar invested in HackerOne, they saved \$15 – with some sectors saving hundreds of millions.

15x

Mitigation Returns

\$81M

Bounties & Bonus Paid

\$3B

Mitigated Loss Savings

9%

YoY Increase in Mitigated Loss Savings

What is
Return on
Mitigation
(RoM)?

RoM is a cybersecurity risk-valuation model that expresses the financial impact of avoided breaches. It combines program data and security spend, with breach cost benchmarks and risk metrics like Single Loss Expectancy (SLE) and Annualized Rate of Occurrence (ARO) to calculate mitigated losses and a RoM multiplier.

Attackers price their campaigns according to the data at risk; bounty values, vulnerability patterns, and program maturity reflect that reality. This year, we focus on four sectors where these dynamics are most visible:

- Financial Services & Insurance (FSI)
- Government
- Retail & eCommerce
- Technology
(*Software, Internet, Crypto, Telecoms*)

Bounty Payouts and Percentage of Critical and High Vulnerabilities by Industry



Figure 22 - Industry insights for bounty payouts (\$) and vulnerabilities (%)

In 2025, Computer Software programs drove the highest payout spend, but only a mid-range share of valid critical and high vulnerabilities (Figure 22).

Telecommunications programs showed the reverse pattern: the lowest overall spend but the second-highest proportion of critical and high findings. Our data suggests that when vulnerabilities are uncovered in this sector, they are disproportionately severe.

This aligns with growing external scrutiny of telecom security, where [policymakers and regulators](#) have flagged the sector's systemic importance and exposure to cascading risks tied to aging telecom infrastructure.

Crypto & Blockchain stands out as having one of the lowest payout spends and the highest number of critical and high-vulnerability assets. This reflects the fact that most activity on the HackerOne Platform to date has focused on Web2-facing assets, underrepresenting Web3 exposures.

Spotlight: Extending into Web3

HackerOne has partnered with Cantina to expand coverage into Web3, connecting customers with leading researchers in smart contracts, blockchain infrastructure, and on-chain systems, bringing the same rigor of coordinated vulnerability discovery to decentralized technologies.

Introducing the ARO and Payload Lenses

ARO per Bug vs. Industry

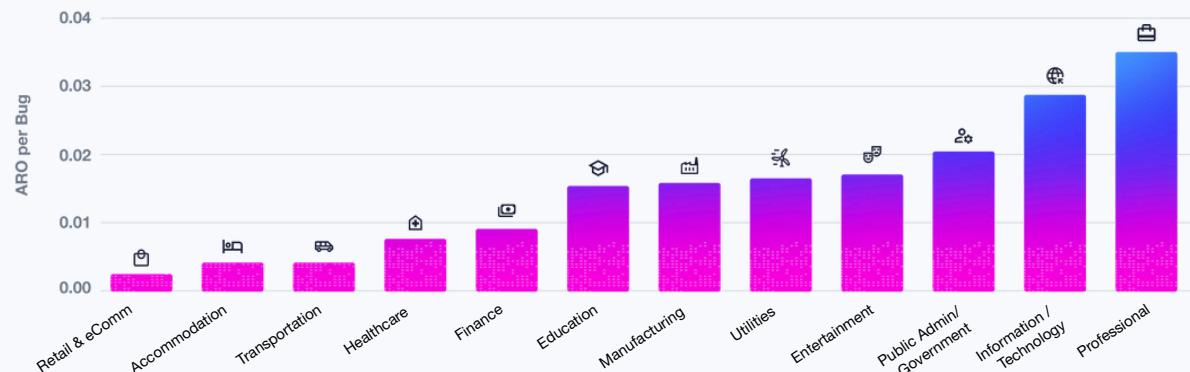


Figure 23 - ARO per bug vs industry, based on Verizon DBIR 2025

This year, our analysis introduces Annualized Rate of Occurrence (ARO), a method of measuring how often a given vulnerability will result in a security incident, to highlight how risk density differs by sector as per [Verizon DBIR](#) (Figure 23).

The sectors that have high report volumes but the lowest ARO per bug, meaning individual issues are less likely to trigger a breach.

This approach accounts for the Incident Response Rate (IRR) we are using in the platform as a global parameter. The IRR adjusts Verizon's numbers for the proportion of actual incidents that get reported through their network.

Government and technology:

Each validated bug carries a disproportionately high chance of cascading into a breach.

Finance:

Fewer but weightier flaws dominate, with direct monetization potential or systemic disruption risk.

Retail and consumer sectors:

These sectors have high report volumes but the lowest ARO per bug, meaning individual issues are less likely to trigger a breach.

This variation feeds directly into our [Return on Mitigation \(RoM\) calculations, which combine Single Loss Expectancy \(SLE\), ARO, and valid vulnerabilities to model avoided loss.](#)

This year, we also introduced a second new lens: the payload analysis initiative. Drawing on over 23,579 redacted vulnerability reports, we cataloged patterns ranging from SQLi probes and XSS vectors to leaked secrets and misconfigured API calls.

While the ARO lens quantifies breach likelihood, payload data surfaces the tactics attackers are actively using, with insights woven throughout the industry sections that follow.

Median, Average, and 95th Percentile Payouts Across Industries in 2025 and Color-coded YoY Changes

	● Critical			● High			● Medium			● Low		
	Median	Average	95th Percentile	Median	Average	95th Percentile	Median	Average	95th Percentile	Median	Average	95th Percentile
🏛️ Government	\$6,500	\$5,500	\$7,750	\$3,000	\$2,545	\$4,000	\$1,000	\$1,000	\$1,680	\$250	\$331	\$662
🏦 Financial Services	\$5,000	\$7,107	\$15,000	\$2,500	\$3,263	\$7,625	\$575	\$575	\$4,000	\$250	\$322	\$1,000
🛍️ Retail & E-commerce	\$5,000	\$6,263	\$20,750	\$2,000	\$2,770	\$6,600	\$500	\$500	\$1,000	\$200	\$212	\$307
💻 Computer Software	\$3,000	\$14,069	\$20,800	\$1,500	\$2,405	\$6,400	\$500	\$500	\$2,250	\$150	\$304	\$938
🌐 Internet & Online Services	\$9,000	\$30,988	\$100,000	\$3,750	\$8,634	\$25,000	\$950	\$950	\$7,499	\$250	\$656	\$2,499
📞 Telecommunications	\$3,000	\$3,667	\$5,600	\$1,500	\$1,778	\$2,600	\$500	\$500	\$847	\$150	\$200	\$412
₿ Crypto & Blockchain	\$60,000	\$488,467	\$2,000,000	\$10,000	\$13,100	\$40,000	\$2,000	\$2,000	\$5,000	\$500	\$457	\$600

Figure 24 - Median, average, and 95th percentile bounty payouts across industries + YoY changes

Between 2024 and 2025, traditional sectors like government, retail, and telco tightened payouts, while digital-first industries, especially internet platforms and crypto, escalated rewards dramatically to attract talent against existential risks. We now see a widening gap between median and top-tier payouts, particularly in crypto, signaling a move toward “pay-for-impact” models where exceptional findings command outsized rewards even as routine bugs are devalued.

The result is a risk-tiered market: cost-optimized industries capping spend versus digital-native industries treating bounties as core defense. For leaders, this means bounties must be treated as a strategic spend, benchmarked against an organization's unique risk profile and brand exposure, not just industry averages.

— Michiel Prins, Co-founder & Senior Director, Product Management at HackerOne

Financial Services & Insurance (FSI)

Risk Picture

Financial institutions remain in the crosshairs of both cybercriminals and nation-state groups. Deepfake-driven Business Email Compromise (BEC), synthetic identity creation, and AI-generated phishing are increasingly bypassing traditional controls. Credential abuse and API exploitation continue to drive intrusions, often through weak access controls in transaction workflows.

The sector's reliance on third-party processors, Know-Your-Customer (KYC) vendors, and APIs compounds supply chain exposure. FSI CISOs are challenged to navigate a complex web of supply chain dependencies, bridging fraud and security teams, and meeting strict regulatory demands.

Strategic Implications

High payouts paired with relatively fewer critical severity findings suggest an industry operating under heightened pressure. High-value findings cluster around authorization bypass, privilege escalation in APIs, and flaws in client-side integrity. RoM data shows consistent efficiency in closing these gaps before adversaries can exploit them.

Recommendations

- Prioritize premiums for findings in authorization logic, session integrity, and authentication workflows to reduce account takeover and fraud risk.
- Expand program scope to cover APIs, mobile apps, onboarding flows, and KYC pipelines: the frontline attack surfaces most exploited in breaches.
- Consider [paying partial bounties](#) for supply chain issues (20% suggested); require processors, KYC/fraud vendors, and SaaS partners to demonstrate regular independent testing and maintain a VDP or equivalent disclosure program.

2025 Program Signals	5X RoM multiplier	\$4M Total Payouts
	\$128M Total mitigation savings	21% High and Criticals

Payload Spotlight

IDOR vulnerabilities consistently escalated to full account takeover in 40-70% of cases. Password reset functionality emerged as the single most dangerous attack vector.

The most common mobile attack paths leveraged WebView and task hijacking. Attackers typically delivered payloads through unvalidated URL loading with JavaScript enabled and improper task affinity configurations. These weaknesses directly enable credential theft, session hijacking, and UI spoofing.

Key programs	Prudential Financial Wells Fargo Goldman Sachs Paypal
---------------------	--

Average cost of a breach	\$5.56M
---------------------------------	----------------

2025 Program Signals

8X	\$1.2M
RoM multiplier	Total Payouts
\$105M	16%
Total mitigation savings	High and Criticals

Payload Spotlight

Researchers frequently submitted authentication bypass payloads in government programs, reflecting the same techniques exploited by state-sponsored groups to gain persistence in identity and cloud collaboration layers.

This is particularly important for government programs, because they often require CAC cards that cannot be credential-stuffed.

Key programs

- [U.S. Department of Defense \(DoD\)](#)
- [U.S. Army and Airforce](#)
- [UK Ministry of Defense](#)

Average cost of a breach

\$2.86M

Recommendations

- Prioritize crowdsourced testing on identity flows and cloud integrations, and coordinate disclosure with identity providers to close high-risk gaps fast.
- Incentivize research on legacy and vendor-integrated platforms.

Government

Risk Picture

Public-sector systems remain prime targets in a year marked by [doubling](#) state-sponsored campaigns like Volt Typhoon and Midnight Blizzard, which exploited identity layers and cloud collaboration tools for persistence.

Governments also contend with a heavy legacy IT burden ([28%](#) of systems are high-risk) and supply chain dependencies that extend exposure beyond their own boundaries. Breach costs aren't measured only in dollars but in mission disruption, diplomatic fallout, and public trust.

Strategic Implications

Government programs show how relatively modest bounty spend delivers amplified risk reduction. Findings cluster around authentication flaws and misconfigurations; weaknesses that map directly to intrusion footholds exploited by ransomware and state-sponsored actors.

- Integrate third-party security into procurement: require suppliers to demonstrate independent assessments and maintain a disclosure policy.
- Build contractual or operational pathways so vulnerabilities in vendor-integrated platforms are surfaced to your teams.
- Establish rapid patch cycles for actively exploited CVEs, treating them as emergencies across IT and security teams.

Retail and E-commerce

Risk Picture

Retailers operate fast-changing estates: web and mobile storefronts, loyalty and checkout systems, POS and fulfillment, and a dense lattice of payment, ad-tech, analytics, and anti-fraud integrations. In 2025 attackers have shown strength in multi-stage intrusions combining credential reuse, session hijacking, and client-side manipulation to monetize at scale.

Magecart-style script tampering at checkout continues to bypass client-side controls and exfiltrate payment data, while recent third-party outages underscored how a single upstream dependency can halt fulfillment and transactions. Groups like Scattered Spider and Shinyhunters highlight the move from site compromise to wider operational disruption across brands and supply chains.

Strategic Implications

Bounty spent in this sector tracks directly to customer trust and brand protection. Payouts concentrate on authentication flaws, exposed admin functions, and insecure integrations with payment gateways and third-party platforms; issues that map to transaction fraud, card theft, and account takeover.

Researchers repeatedly surface these flaws at scale, mirroring attacker monetization patterns. RoM results confirm outsized savings, making bug bounty one of the most efficient security controls in a low-margin, high-risk sector.

Recommendations

- Pay premiums for findings tied to customer trust and fraud vectors: session hijack, weak recovery flows, loyalty/gift-card API bypasses, and client-to-server data leaks enabling skimming.
- Scope client-side integrity explicitly. Treat third-party scripts and browser supply chains as first-class assets.

2025 Program Signals **7.4X** **\$5.7M**
RoM multiplier Total Payouts

\$144M **40%**
Total mitigation High and Criticals savings

Payload Spotlight

Thousands of submissions featured script injection and skimming payloads, echoing Magecart-style compromises of checkout pages. Researchers also deployed session replay and token manipulation techniques to probe loyalty and gift-card APIs, mirroring the fraud monetization routes favored by threat actors.

The bounty data aligns almost one-to-one with attacker tradecraft. The same payloads fueling active cybercrime campaigns, Magecart skimmers, and loyalty token abuse, are surfacing in researcher submissions, underscoring how closely hacker findings track with real-world exploitation.

Key programs

- [A.S. Watson](#)
- [Shopify](#)
- [Lowe's](#)
- CapitalOne ([VDP](#) / [Bounty](#))
- [John Deere](#)

Average cost of a breach

\$3.54M

- Embed supply chain security into procurement: require gateways, KYC/fraud vendors, tag managers, and POS/OMS providers to show evidence of regular testing and coordinated disclosure processes.
- Prioritize submissions that demonstrate plausible fraud paths (e.g., loyalty cash-out, coupon abuse, refund loops) with clear linkage to fraud KPIs. Require safe PoCs rather than live exploitation.
- Ahead of peak events, run focused testing campaigns on checkout, inventory, and pricing systems to reduce high-traffic exposure windows.

2025 Program Signals

23X

RoM
multiplier

\$20M

Total
Payouts

\$1.7B

Total mitigation
savings

24%

High and
Criticals

Payload Spotlight

Payloads clustered around XSS vectors, JWT manipulations, and misconfigured API probes. For crypto and blockchain, wallet key-related payloads and signing flow tests stood out.

The connective thread is trust boundaries being mishandled across high-velocity release cycles, a structural flaw that attackers monetize fastest.

Key programs

- [Anthropic](#)
- [OKG](#)
- [Adobe](#)
- [Coinbase](#)
- [Salesforce](#)
- [Crypto.com](#)
- [Zoom](#)
- [AT&T](#)

Average cost of a breach

Technology:
\$4.79M

Communications:
\$3.75M

Recommendations

- Incentivize high-value flaws by subsector:
 - Software & SaaS: Cross-tenant isolation, API exploits.
 - Internet platforms: Access controls and exposed admin surfaces.
 - Crypto: Wallet signing and custody flows.
 - Telcos: Identity/authentication layers.
- Pair AI-assisted secure code reviews with continuous crowdsourced testing to catch insecure AI-generated code before release.

Technology:

Computer Software, Internet & Online, Cryptocurrencies and Blockchain, Telco

Risk Picture

Over the past eight years, technology companies have generated more valid vulnerability reports on HackerOne than any other sector:

AI-assisted coding and automation accelerate delivery but also reintroduce vulnerabilities like XSS and injection at scale.

Internet and SaaS platforms struggle to enforce consistent access controls in high-velocity release cycles, leaving IDOR, privilege escalation, and exposed administrative functions as recurring findings.

In crypto and blockchain, 2025 has already seen [\\$2.17B in global losses](#), with breaches tied to misconfigured APIs, weak key management, and outdated dependencies.

Telcos face growing systemic risk, with attackers increasingly targeting identity and signaling layers as entry points into national infrastructure and supply chains.

Strategic Implications

Vulnerability submissions remain dominated by XSS, authorization bypass, and misconfigurations in high-velocity release cycles. However, the stakes diverge sharply, from billions lost in crypto breaches to user trust erosion in SaaS.

HackerOne program data shows this cluster consistently delivers the highest RoM multipliers across industries.

- For crypto, enforce strict wallet key management and require external red-teaming of signing flows and custody models.
- In telecom, focus testing on identity/authentication exposure and customer account recovery flows.
- Run coordinated testing campaigns on high-value APIs tied to transactions, customer data, and integrations, with premiums for authentication bypasses and misconfigurations.

Closing Remarks

2025 marks a formative moment in the evolution of vulnerability discovery.

The arrival of hackbots on the platform signals the beginning of a new phase for crowdsourced security: one where AI-driven automation acts as a force multiplier.

What is emerging is the bionic hacker: individuals who pair deep technical expertise with AI capabilities to accelerate recon, streamline triage, and focus their energy on the complex flaws that matter most. Those who embrace AI gain leverage, while organizations that enable this model see richer, faster, and more impactful findings.

For CISOs, adversarial pressure is now both continuous and augmented. Attackers are blending automation with scale, probing at machine speed and exploiting exposures before defenders can react.

The most resilient organizations mirror this dynamic: incorporating continuous offensive testing programs that combine structured pentests for compliance and speed, bug bounty and disclosure programs for continuous breadth, and adversarial AI system testing for emerging risks. What differentiates successful leaders is prioritizing what matters most in their business context – adopting an adaptive exposure management discipline.

HackerOne remains deeply engaged in this transformation. Our commitment to transparency, fairness, and progress is unchanged. ***As the lines between human and machine blur, we believe the future of security lies in collaboration, not competition.*** By equipping researchers and security teams to responsibly harness AI, we move toward a future that is more adaptive, more resilient, and fundamentally more secure.

hackerone | Global leader in offensive security.

Our HackerOne Platform combines AI with the ingenuity of the world's largest community of security researchers to find and fix security, privacy, and AI vulnerabilities across the software development lifecycle. The platform offers bug bounty, vulnerability disclosure, pentesting, AI red teaming, and code security. We are trusted by industry leaders like Anthropic, Crypto.com, General Motors, GitHub, Goldman Sachs, Uber, and the U.S. Department of Defense. HackerOne was named a Best Workplace for Innovators by Fast Company in 2023 and a Most Loved Workplace for Young Professionals in 2024.

To turn these report results into action, [contact HackerOne today](#).

Data Sources and Methodology

HackerOne Platform Data

- **YoY Timeframe:** July 1, 2024 – June 30, 2025.
- **Scope:** All HackerOne customer programs active during the reporting period.
- **Normalization:** Data was aggregated and anonymized across industries, regions, and program types to preserve customer confidentiality while surfacing broad trends.

Customer Survey

- **Scope:** HackerOne customers across maturity levels and industries.
- **Method:** Independent survey conducted by UserEvidence between June 1 and August 25, 2025.
- **Sample Size:** 99 respondents globally. The sample included 6% Fortune 500 companies, 43% large enterprises, and 31% executives or senior managers, with representation across industries.

Researcher Survey

- **Scope:** Active HackerOne researchers who have submitted at least one valid vulnerability report since June 1, 2024. Customer-specific or confidential data was excluded.
- **Method:** Online survey conducted via Intercom between July 14, 2025 and August 8, 2025.
- **Sample Size:** 1,825 respondents.
- **Data Defensibility:** For each question, all calculations (counts and percentages) are based only on the number of valid responses for that specific question, excluding any non-responses to ensure accuracy. Multi-select questions were parsed to count each selected option individually.

Payload Analysis

This year, we conducted a payload analysis of over 45,000 payload signatures across **23,579 redacted vulnerability reports** submitted between **July 1, 2024, and June 30, 2025**. These reports span web applications, mobile platforms, cloud infrastructure, and language-specific frameworks. Reports were selected from validated findings across HackerOne programs and compiled by our data team to provide actionable insights.

External Benchmarks

- [Verizon Data Breach Investigations Report \(DBIR\) 2025](#)
- [IBM Cost of a Data Breach Report 2025](#)
- [SANS 2024 Top Attacks and Threats Report](#)
- [2024 ISC2 Cybersecurity Workforce Study](#)
- Policy documents and regulatory advisories (including U.S. Congressional Research Service briefs, OWASP AI Exchange, NIST AI RMF, and NYDFS guidance on AI security)
- Security news coverage and incident reporting highlighting key breaches and industry responses

Methodological Notes

- **Return on Mitigation (RoM):** RoM, a HackerOne developed methodology, is calculated using IBM's reported average breach costs as a baseline for Single Loss Expectancy (SLE). Platform data and Verizon DBIR on validated vulnerabilities and Annualized Rate of Occurrence (ARO) provide inputs for avoided loss estimates.
- **Bias Controls:** Only validated vulnerabilities are included in aggregate counts.
- **Expert Oversight:** This report was produced in collaboration with HackerContent, uniting HackerOne's expert data team with independent expertise from HackerContent Director Luke Stephens and contributor Jessica Williams.

To turn these report results into action, [contact HackerOne today](#).