Six must-know ethical hacking facts and stats for businesses

BY ANNA HAMMOND · JULY 3, 2024 · LAST UPDATED ON MARCH 6, 2025

The role of ethical hackers in cybersecurity teams has become more crucial than ever. With the increasing complexity and frequency of cyber threats, organizations must adopt proactive measures to protect their digital assets and infrastructure. Ethical hackers provide invaluable insights into potential vulnerabilities and the latest hacking techniques due to their deep understanding of how attackers operate.

By simulating real-world attacks, ethical hackers, also known as security researchers, help organizations identify and rectify security weaknesses before malicious hackers can exploit them. This preemptive approach prevents data breaches and financial losses and safeguards an organization's reputation.

Furthermore, ethical hackers play a crucial role in compliance. Organizations promptly address vulnerabilities and ensure systems meet regulatory standards, avoiding potential legal and financial consequences. This proactive approach not only strengthens security but also showcases an organization's dedication to safeguarding sensitive data under regulatory guidelines.

For a more detailed analysis of the current ethical hacking landscape, download The Ethical Hacker Insights Report 2024. Alternatively, keep reading for a preview of six valuable insights from the report.

1. Crowdsourced security testing adoption is accelerating

Crowdsourced security testing, such as bug bounty programs, has become as mainstream as traditional testing methods. This method not only enhances security posture but also accelerates the identification and remediation of security flaws. As a result, crowdsourced testing is now a critical component of comprehensive security strategies in organizations worldwide.

This shift is driven by the dynamic nature of cyber threats and the need for diverse, innovative approaches to security. Carles Llobet, Senior Security Engineer at Personio, agrees:

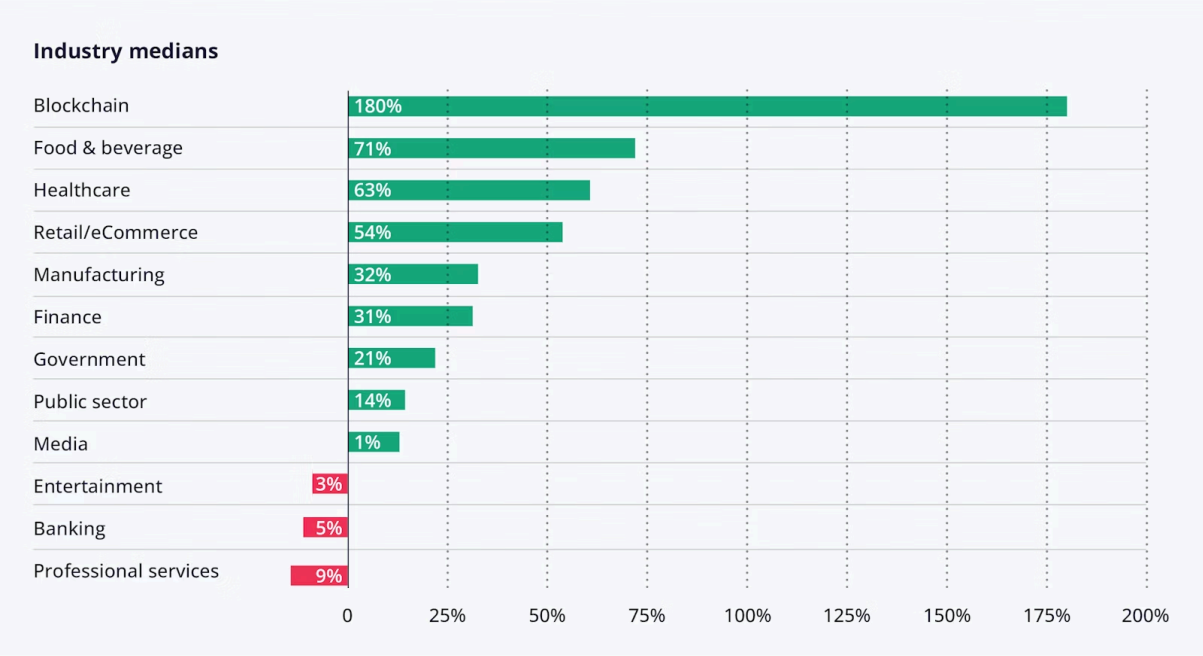
> *""Having a bug bounty program not only helps to fix all of these findings and improve overall security posture but also speaks highly on how organizations treat matters as important as security.""*

This method has become a staple in cybersecurity strategies, with major brands like Microsoft, Nestlé, Coca-Cola, and Monzo already leveraging ethical hacking communities through bug bounty programs. Their buy-in is a testament to the established value of ethical hacking communities, a reputation that's grown significantly over the last five years.

2. Average bug bounty payments have doubled

Bug bounty programs incentivize external security researchers to identify vulnerabilities, offering substantial rewards for critical findings. The success of these programs is evident in the escalating bounty payouts. Intigriti analyzed the data from 640 bug bounty tables as part of the Ethical Hacker Insights Report. Compared to March 2023, the average bounty reward has doubled, while the median bounty amount increased by 13%.

The increases in bounty rewards across various industries reflect evolving cybersecurity priorities. In blockchain, established players are doubling down on their programs, resulting in a 180% increase in rewards. Many food and beverage companies are also increasing the median bounty payout after cleaning up the low-hanging fruit of lower-severity vulnerabilities. Healthcare has seen significant buy-in from larger players, boosting budgets and resulting in a 63% increase. Government programs are expanding as digitalization increases the industry's scope, contributing to a 21% growth.



Bug bounty median payouts

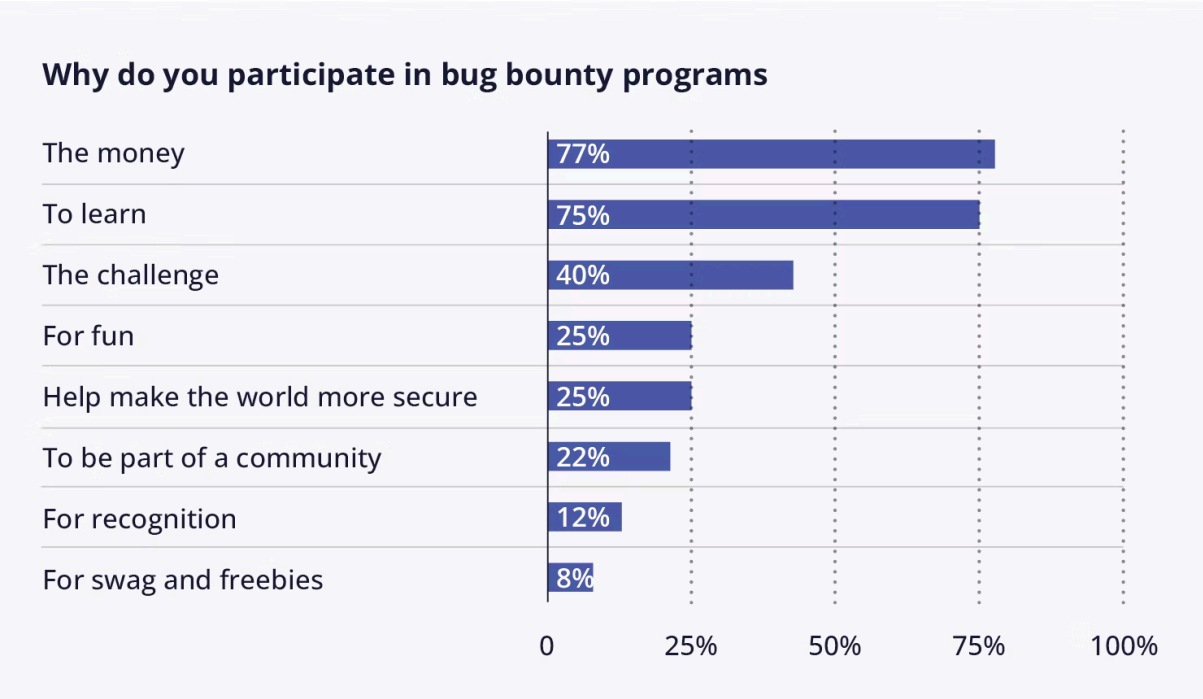
The growing adoption of ethical hacking is a sign of a shift toward proactive cybersecurity strategies and away from a reactive approach to dealing with sophisticated cyber threats. By ensuring regulatory compliance and protecting sensitive data, businesses can gain a competitive advantage and build trust with customers and stakeholders.

3. Financial incentives are the primary motivator for ethical hackers

Financial gain remains the primary motivator for 77% of ethical hackers. This incentive attracts a large pool of talented individuals to the field and encourages them to continuously hone their skills. Further, the opportunity to earn motivates ethical hackers to diligently probe and test software and systems for security weaknesses. This financial motivation ensures that organizations benefit from top-tier expertise and proactive security, making bug bounty programs effective in strengthening cyber defenses.

4. Bug bounty programs are an educational powerhouse

Bug bounty programs aren't just about earning bounties; they're also a significant educational resource for ethical hackers. With 75% of ethical hackers using these platforms to learn, these programs are vital for skill development and staying current with emerging security threats.

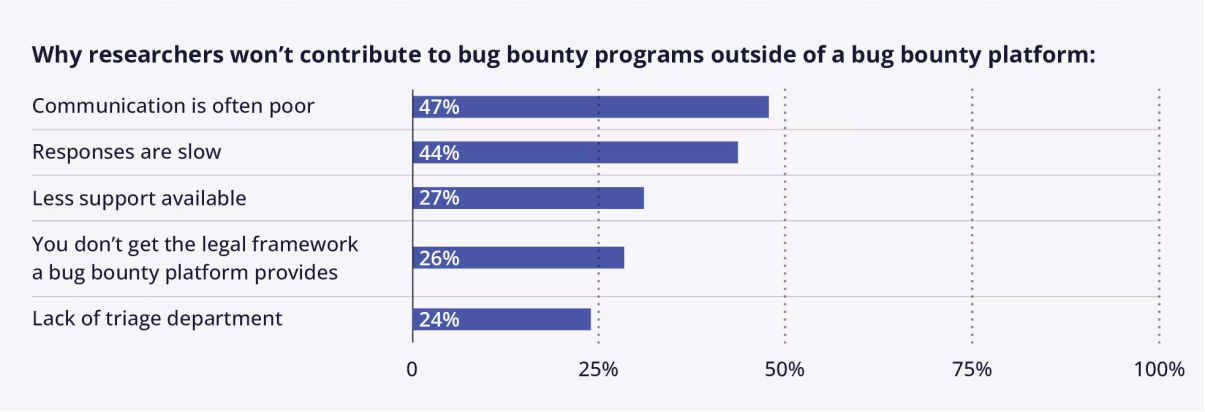


The strength of the ethical hacking community lies in its diversity, offering a broad spectrum of problem-solving approaches. These professionals come from various professional backgrounds, such as information technology, computer science, and cybersecurity. Some may specialize in web application vulnerabilities, while others focus on network security or social engineering. This range of expertise ensures that businesses can access the precise skills required for their cybersecurity goals.

5. Preference for structured bug bounty platforms

A significant portion of the community, 40%, prefers to refrain from engaging with bug bounty programs not hosted on structured platforms, like Intigriti.

The preference for structured bug bounty platforms is well-founded. Unstructured programs often suffer from slow response times, poor communication, and a lack of transparency. These factors can significantly hinder the efficiency of ethical hacking efforts and discourage participation.



In contrast, structured platforms address these concerns by providing clear guidelines, streamlined communication channels, and regular updates on bug reports and rewards.

Structured bug bounty platforms offer more than just operational efficiency and improved communication. They're designed to build trust and respect between ethical hackers and the organizations they support. When ethical hackers feel valued and respected, they're more likely to contribute their expertise and knowledge, leading to more comprehensive and effective vulnerability assessments.

Organizations seeking to engage ethical hackers should strongly consider the benefits of bug bounty platforms. These platforms attract top talent and maximize the effectiveness of ethical hacking initiatives. They provide a framework that fosters collaboration, transparency, and efficiency, ultimately enhancing an organization's overall cybersecurity posture.

6. Retesting is critical for robust security

Organizations must be more vigilant than ever to protect themselves from an evolving threat landscape. Retesting is a critical part of this defense. Beyond its role as a validation tool, retesting provides deep insights into an organization's security posture, enabling informed decision-making and proactive threat mitigation.

In addition, retesting plays a critical role in demonstrating compliance with industry regulations and standards. As data protection mandates become more stringent, retesting provides clear evidence that an organization is committed to maintaining compliance.

Intigriti's survey found that an overwhelming 95% of ethical hackers are likely to retest a vulnerability they reported if asked. This practice is crucial as it ensures that the remediations are effective and that no new issues have arisen, thereby maintaining a robust security posture.

Want to learn more about ethical hacking communities?

Intigriti collected the responses of 550+ security researchers during April 2024. As mentioned, we also analyzed more than 640 bug bounty tables across multiple industries to help organizations benchmark against their industry peers and make an informed decision about how to reward security researchers for reporting vulnerabilities.

To continue learning about this important cybersecurity community, download The Ethical Hacker Insights Report 2024 today.

REQUEST A DEMO	VISIT THE WEBSITE	GET IN TOUCH
intigriti.com/demo	intigriti.com	hello@intigriti.com