SANS | Research Program

White Paper

Human-Powered Security Testing

Written by **Matt Bromiley**

August 2024

hackerone

Executive Summary

The current proliferation of cyber threats is not a problem that can be ignored. In 2023, the average cost of a data breach reached an all-time high of $4.45 million, a 15.3% increase from 2020.[1] Organizations continue their best attempts to stay vigilant, defending against a range of attacks from ransomware to phishing to vulnerability exploits to credential harvesting and more. Needless to say, it's a minefield that requires careful and consistent testing to ensure that defenses are at their best.

As cyber threats grow in sophistication and frequency, organizations must stay ahead by identifying and mitigating vulnerabilities before adversaries can exploit them. In a 2023 SANS survey, approximately 39% of respondents lacked confidence that they understood their threat exposure.[2] Although automated tools certainly have their place and are useful, they fall short in replicating the ingenuity and adaptive strategies of human attackers. Reports over the past five years have shown that as many as 84% of tested companies continue to have high-risk vulnerabilities exposed on their network.[3]

This is where human-powered security testing provides a critical advantage.

Human-powered security testing leverages the skills of experienced security professionals to uncover hidden vulnerabilities and simulate real-world attack scenarios. Human testers bring creativity, intuition, and a deep understanding of evolving threat landscapes and tools. Organizations can harness this knowledge to proactively identify weaknesses and bolster their defenses.

Discussing human-powered security is one thing. However, where are organizations seeing actual returns? How do we evaluate returns on security investments? In this white paper, we will explore return on mitigation (ROM), as opposed to typical return on investment (ROI), for investment evaluations. Furthermore, we'll examine the tangible benefits of human-powered security testing through real-world examples and testimonials from three key industries:

- Financial services
- Retail/e-commerce
- Online services/computer software

Human-powered security control testing can seem daunting at first, because automated tools can offer a "set it and forget it" approach. However, this does little to help actively engage and test a security team, who must deal with a changing landscape that automated tools may not be able to emulate.

As you work your way through this white paper, you will gain insights into how human-powered security testing can significantly enhance your organization's security posture. We will outline the steps necessary to integrate these services into your existing security strategy, discuss how to build internal support for their adoption, and highlight the evaluation mechanisms to find value in your security posture.

---

[1] "101 of the Latest Data Breach Statistics for 2024," https://secureframe.com/blog/data-breach-statistics

[2] "Building a Resilient Offensive Security Strategy," www.sans.org/white-papers/building-resilient-offensive-security-strategy

[3] "Cybersecurity vulnerability (CVE) statistics and facts (2019–2024)," www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics

Human-Powered Security Testing

The evolving nature of cybersecurity threats necessitates a proactive and adaptive approach to security testing. CrowdStrike's 2024 Global Threat Report noted that some threat actors, particularly eCrime, can achieve breakout times of *less than three minutes*.[4] This simply isn't enough time for defenders to hopefully "catch" the bad guys in action.

Human-powered security testing is a powerful method for uncovering vulnerabilities that might not be caught by automated tools and traditional testing methods. Furthermore, humans can better emulate *other* humans—aka, adversaries. One of the cornerstone implementations of human-powered security, bug bounty programs, crowdsources security testing to a group of highly skilled security researchers. In the "SANS 2024 Application Security and API Survey,"[5] respondents found value in bug bounty programs in every area of application testing, including:

- Single-page web applications
- Native mobile applications
- SOAP APIs
- Representational state transfer (REST) APIs

Let's look at some of the key, high-level areas where human-powered security offers strategic benefits.

Industry Perspective

"The community is a force for good. Partnering with ethical hackers helps us build increased resilience and confidence in our product security posture because more eyes on our products translates to better coverage."

—Product Security Manager, Internet and Online Services

Benefits of a Human-Powered Security Team

Human-powered security testing excels in advanced threat detection by emulating real-world attacks and adversaries. Human testers can think and act like adversaries, uncovering entry vectors and vulnerabilities that automated tools might miss. This provides a much more comprehensive assessment of an organization's security posture.

Many organizations have already realized the benefits of human-powered security testing—even if they don't think of it as such. In 2023, SANS and HackerOne found that the top four offensive or proactive security measures were largely human-driven or required human interpretation.[6] Human testers continuously adapt to new threats. They can utilize their ingenuity to find creative ways to penetrate systems.

Human-powered security programs can also rely on a global network of *other* humans. Unlike static, automated tools, the diversity and creativity of a global community of security researchers bring a broader perspective to security testing. This continuous adaptation ensures that organizations stay ahead of evolving threats, making human-powered security testing a vital component of a holistic security strategy.

Human-powered security testing provides an integrated approach to cybersecurity, ensuring continuous monitoring and testing. This integrated approach delivers the type of ROI that stakeholders seek when developing their security testing programs.

---

[4] "CrowdStrike 2024 Global Threat Report," www.crowdstrike.com/global-threat-report

[5] "SANS 2024 Application Security & API Survey: Protecting our Applications and APIs," June 5, 2024, www.sans.org/white-papers/sans-2024-application-security-api-survey-protecting-our-applications-apis

[6] "Building a Resilient Offensive Security Strategy," www.sans.org/white-papers/building-resilient-offensive-security-strategy

Increasing Confidence in Adopting Human-Powered Security Services

For decision-makers, adopting human-powered security testing could seem intimidating initially. However, understanding its tangible benefits and proven effectiveness can significantly boost confidence in embracing these services. Investing in human-powered security brings a nuanced perspective that automated tools alone cannot provide. Human-powered services excel in understanding context and prioritizing business-critical vulnerabilities, which enables better strategic decision making.

Transparent reporting and actionable insights from human-powered security testing help decision makers understand specific risks and prioritize mitigation efforts. Emphasizing the concept of return on mitigation (ROM) as an alternative to traditional ROI can highlight the financial benefits of proactive security measures. ROM compares the potential costs of a breach with the investment in mitigation strategies, demonstrating the economic advantages of robust security testing. We'll explore ROM more in the next section.

Industry Perspective

"The findings from the program help enhance our preventative security efforts from the inside out. Our engineering team reviews each report, prioritizes according to the severity, and uses the data to better understand and protect against malicious hackers. From an ROI perspective, bug bounty is one of the most effective programs in our security strategy."

—VP of Program Management, Enterprise Cloud Services

Building a Case for Human-Powered Security Programs Internally

Gaining internal support for human-powered security testing requires a strategic approach. Security leaders must articulate the value and necessity of these programs effectively. Showing how they have helped other organizations avoid breaches and mitigate risk can drive compelling adoption.

Acknowledging the business aspects of security investments also frames human-powered security programs in a digestible manner, highlighting the benefit to the organization—not just the security team. In this white paper, we'll look at the idea of ROM vs. ROI. The unique ability of skilled security professionals to mitigate complex vulnerabilities and deliver context-driven value, coupled with ROM, makes a compelling business case.

Security Control Testing Insights

Robust security control testing is indispensable for identifying and mitigating risk before it can be exploited by malicious threat actors. We'll next dive deeper into various security assessment methodologies, including red teaming and bug bounty programs, along with the concept of ROM as a practical framework for evaluating the effectiveness of security investments.

Red Teaming in Security Assessments

Red teaming plays a critical role in comprehensive security assessments by simulating real-world attack scenarios. Unlike traditional penetration testing, which focuses on identifying specific vulnerabilities, red teaming aims to test the organization's overall defense mechanisms and response capabilities. This is done by mimicking the tactics, techniques, and procedures (TTPs) of threat actors known to be active or targeting your organization.

Red teaming also may pair up with the organization's blue teams, to establish "purple teaming" operations. This approach actively tests the defenders while the red team seeks ways to evade detections and security controls.

Industry Perspective

"[With security testing programs], you don't have a return on investment, you have a return on mitigation/ prevention. You can quantify what a breach will cost. You can then give that a cost in terms of impact on the business (reputation, data loss, revenue). Business understands the return on prevention."

—Head of Cybersecurity, Financial Services Provider

Bug Bounty Programs Complement Security Testing

Bug bounty programs complement red teaming efforts by leveraging the collective expertise of a global community of ethical hackers. These programs incentivize security researchers to identify and report vulnerabilities, providing continuous and diverse testing perspectives. The "always-on" nature of bug bounty programs ensures that security testing keeps pace with the rapid evolution of cyber threats.

Whereas red teaming offers a strategic overview of security resilience, bug bounty programs focus on specific vulnerabilities. This introduces creativity and ingenuity to the testing process. Together, these two approaches provide well-known methods for testing and assessing an organization's weaknesses.

Beyond immediate cost savings, bug bounty programs offer several qualitative benefits that enhance an organization's security posture:

- **Continuous improvement—**The ongoing nature of bug bounty programs fosters a culture of continuous improvement and vigilance between organizations and the security researcher community.
- **Diverse perspectives—**Engaging a global community of researchers brings diverse perspectives and innovative solutions to security challenges.
- **Reputation management—**Demonstrating a commitment to proactive security through bug bounty programs enhances an organization's reputation and builds trust with its customers and stakeholders.

Cost-Benefit Analysis: ROI vs ROM

When seeking budget for implementation or security posture justification, we have been taught to rely on typical ROI calculations. However, quantifying the ROI for security control testing can be challenging due to the intangible nature of cybersecurity benefits. For example, did the technology in place effectively stop a data breach that could have resulted in material impact? How can we know what every spear phish will lead to?

Traditional ROI calculations often fall short in capturing the full value of security investments. Gaining traction as an alternative assessment mechanism is ROM, which compares the anticipated costs of a security breach with the costs of implementing mitigation strategies. It provides a more nuanced understanding of the financial benefits of proactive security measures. ROM factors in various potential costs, including:

- Restoring compromised systems
- Lost revenue due to downtime
- Legal and regulatory penalties
- Damage to public trust and reputation

By assessing the effectiveness of mitigation strategies in terms of potential financial consequences, ROM offers a practical framework for stakeholders to evaluate the value of security investments. It also shifts the focus from immediate cost savings to long-term resilience, with a magnifying glass on risk management.

ROM is also more flexible to accommodate for the growing nature and impact of cyber threats. For example, the average cost of a data breach changes annually, based on new statistics, attack methods, and adversary motivations. A significantly impactful piece of ransomware or a breach of SolarWinds magnitude could cause a shift in global averages. ROM helps to better quantify this changing landscape compared to traditional calculations such as inflation or depreciation.

Industry Perspective

"The bug bounty program is the highest ROI across all of our spend. It's really hard to show ROI, but with bug bounty, I have a baseline. I can say, 'This vulnerability was able to be found by someone outside the organization. Someone that was not authorized to access this system was able to access it.' Even with vulnerabilities that are not within our program, bug bounty allows me to put a price tag on them. I can explain this business case and our stakeholders are able to prioritize bug bounty higher than other tools that also generate ROI."

—Head of Application Security, Online Travel Agency

ROI vs. ROM Case Study

To illustrate the practical benefits of human-powered security testing and calculations of ROI vs. ROM, consider a case study from the financial services sector. A major financial institution implemented a bug bounty program alongside its existing red teaming efforts. Over the course of a year, the program identified several critical vulnerabilities that had been overlooked by previous tests.

Scenario

- **Initial security investment—**The institution invested $200,000 in the bug bounty program and an additional $100,000 in red teaming exercises.
- **Potential breach costs—**A potential breach was estimated to cost the institution $5 million, including costs associated with restoring compromised systems, lost revenue, legal penalties, and reputational damage.

Return on Investment (ROI)

A simple ROI calculation looks at the return of $300,000 against a potential $5 million breach.

- **Breach prevention—**By identifying and mitigating vulnerabilities, the institution avoided a potential $5 million breach.
- **Cost of testing—**The total investment in proactive security testing was $300,000.

Using Traditional ROI Calculations

Traditional ROI or cost-benefit analyses yield approximately $15.67 in ROI.

$$\text{ROI} = \frac{\text{Benefit} - \text{Cost}}{\text{Cost}} = \frac{\$5{,}000{,}000 - \$300{,}000}{\$300{,}000} = \frac{\$4{,}700{,}000}{\$300{,}000} = \$15.67$$

If we look at ROM, we compare the cost of implementing security measures against the anticipated breach cost.

$$\text{ROM} = \frac{\text{Anticipated Breach Cost}}{\text{Mitigation Cost}} = \frac{\$5{,}000{,}000}{\$300{,}000} = \$16.67$$

In this scenario, the ROM indicates that for every dollar spent on mitigation, the organization potentially saves $16.67 in breach costs. For the sake of this case study, we kept these costs simple. However, it is important to remember that breach costs these days include much more than just a simple flat dollar amount. They also include potential ransom payments, compliance requirements, regulatory fines, legal fees, brand damage, and much more.

Far too many organizations unlock their security budget after a breach occurs. Unlocking a proactive budget is not an easy feat for security leaders and executives with traditional evaluation mechanisms. ROM is a better assessment of the value a security program provides, which can empower executive discussions and cement security priorities before a breach occurs.

Case Studies: The Value of Bug Bounty Programs Across Industries

The implementation of bug bounty programs has provided appreciable value across various industries. These programs have enabled organizations to uncover critical vulnerabilities, enhance their security posture, and build trust with their stakeholders. For this white paper, HackerOne sourced feedback from customers in three key industries:

- Financial services
- Retail/e-commerce
- Online services/computer software

The following is a high-level summary of the key findings and the benefits experienced by these organizations.

Financial Services

Key Challenges

Financial services are often targeted by state-nexus threat actors for espionage and financial disruption. Aside from managing large amounts of money, financial services often also provide key services for millions of users. These databases and applications are often the target of identity theft and fraud attacks. Per the "SANS 2023 Attack and Threat Report," financial services experienced 70 compromises in Q1 of 2023, with approximately 1.7 million victims.[7]

Advantages of Human-Powered Security

Organizations in the financial services sector, including leading global banks and financial technology companies, have reaped substantial benefits from bug bounty programs. These programs have proven instrumental in identifying vulnerabilities that traditional security measures might miss.

The average tenure for these programs is 4.3 years.

Key Findings

- **Enhanced threat detection:**
  - Bug bounty programs enabled financial institutions to emulate real-world attack scenarios, uncovering critical vulnerabilities that automated tools and traditional security testing failed to detect.
  - Continuous engagement with a global community of ethical hackers provided diverse and innovative insights into potential security gaps.
- **Improved security posture:**
  - Financial institutions invested in both public and private bug bounty programs, leading to the discovery and mitigation of vulnerabilities in their financial applications.
  - These efforts resulted in strengthened defenses against sophisticated cyber threats, reducing the risk of financial fraud and enhancing overall security.
- **Financial impact:**
  - The proactive identification of vulnerabilities helped these organizations avoid significant breach costs, which could amount to millions of dollars in potential financial losses, legal penalties, and reputational damage.
  - By comparing the costs of implementing bug bounty programs to the potential breach costs, organizations demonstrated a high ROM, validating the prudence of these investments.

Industry Perspective

"In the board meeting this week, our CISO quoted number of submissions and criticals we received this year. Said these were near misses from a breach perspective. The ability to package it and have it supported from a third party coupled with an unbiased hacker is incredibly valuable and a highlight of our security program."

—Head of Threat Management, International Insurance Group

[7] "SANS 2023 Attack and Threat Report," June 26, 2023, www.sans.org/white-papers/sans-2023-attack-threat-report

Retail/E-Commerce

Key Challenges

Retail and e-commerce platforms, like financial institutions, provide essential services of economic and payment value to millions of users. Their databases and transaction history are prime targets for adversaries, along with the underlying software. Supply chain attacks are common, because today's modern e-commerce platforms often rely on an amalgamation of third-party services and products, rather than being entirely homegrown. These platforms are also highly susceptible to disruptive attacks that can impact business operations.

According to the "SANS 2023 Attack and Threat Report," retail experienced 16 compromises in Q1 2023 with an approximate victim count of 170,000.[8]

Advantages of Human-Powered Security

Retail and e-commerce companies have found value in bug bounty programs, which have played a crucial role in protecting customer data and ensuring the security of online transactions.

The average tenure for these programs is 5.6 years.

Industry Perspective

"Specific findings of hackers enabled us to build a new secure code training program for our development teams. This program has helped us increase the quality of the code and reduce vulnerabilities. It's also increased our prevention capabilities by shifting left as much as possible to secure the SDLC. We noticed a decrease in total valid reports over the years, and we lowered costs by remediating issues in live environments."

— CISO, Health and Beauty Retailer

Key Findings

- **Customer data protection:**
  - Bug bounty programs helped identify vulnerabilities in e-commerce platforms, ensuring that customer data was protected from potential breaches.
  - Continuous security assessments provided by ethical hackers enhanced the overall security of these platforms.
- **Transaction security:**
  - By uncovering and addressing critical security issues, retail and e-commerce companies were able to secure online transactions, fostering greater customer trust.
  - The programs offered an always-on approach to security testing, keeping pace with the rapid evolution of cyber threats.
- **Operational efficiency:**
  - The findings from bug bounty programs allowed these companies to implement effective mitigation strategies, reducing the risk of downtime and financial losses due to security incidents.
  - The qualitative benefits included improved security culture within the organizations and heightened awareness of cybersecurity best practices.

[8] "SANS 2023 Attack and Threat Report," June 26, 2023, www.sans.org/white-papers/sans-2023-attack-threat-report

Online Services/Computer Software

Key Challenges

Given their placement in software supply chains and as integral third parties for *many* industries, online services and computer software providers are a prime target for advanced, sophisticated threat actors. Gaining a foothold in a company can potentially expose dozens or hundreds more, as we saw in recent breaches such as SolarWinds and Snowflake. These industries are also susceptible to insider threats and vulnerability exploitation.

According to the "SANS 2023 Attack and Threat Report," the technology sector suffered 33 breaches with an approximate victim count of 22.3 million.[9]

Advantages of Human-Powered Security

Companies in the online services and computer software sectors utilize bug bounty programs to ensure the safety and reliability of their platforms.

The average tenure for these programs is 8.3 years.

Key Findings

- **Platform security:**
  - Bug bounty programs helped uncover critical vulnerabilities in software development tools and online service platforms, ensuring that these environments remained secure.
  - Continuous engagement with security researchers provided a diverse range of insights, helping to address security flaws comprehensively.
- **Trust and safety:**
  - The proactive identification and mitigation of vulnerabilities enhanced the trust and safety of users, developers, and customers interacting with these platforms.
  - Companies were able to demonstrate their commitment to security, thereby building stronger relationships with their stakeholders.
- **Innovation and adaptability:**
  - By leveraging the ingenuity of a global community of hackers, these companies continuously adapted their security measures to address emerging threats.
  - The programs fostered a culture of innovation, where security improvements were consistently integrated into the development life cycle.

Across these various industries, bug bounty programs have proven to be invaluable. They have enabled organizations to proactively identify and address vulnerabilities, ensuring robust protection against evolving cyber threats.

[9] "SANS 2023 Attack and Threat Report," June 26, 2023, www.sans.org/white-papers/sans-2023-attack-threat-report

Conclusion

As organizations face increasingly sophisticated cyber threats, adopting a comprehensive security strategy that aligns with long-term business objectives is crucial. Automated tools alone are insufficient to address the complex and evolving nature of these threats. There is simply too much nuance and context for automated tools to effectively cover. Human-powered security testing provides the insights and understanding needed to identify and remediate vulnerabilities effectively, fostering a culture of continuous improvement and vigilance within organizations.

By integrating human expertise with advanced technology, organizations can enhance their security posture and protect critical assets. This dual approach not only mitigates risks but also ensures compliance with industry regulations, which is vital for maintaining customer trust and achieving a competitive advantage. Regular human-powered security assessments demonstrate a commitment to security that resonates with stakeholders and strengthens the organization's reputation. Further, it's been found that companies that are up front with their security risks and mitigate them find greater customer success.

Finally, investing in human-powered security testing offers strategic value beyond immediate threat mitigation. It supports long-term business objectives by aligning security measures with regulatory compliance, enhancing customer confidence, and positioning the organization as a leader in cybersecurity. In this white paper, we examined the concept of return on mitigation vs. return on investment as a cultural shift, focusing on how security investment can save an organization significant sums, rather than assessing how much money the tool has generated.

By fostering a proactive security culture and continuously evolving to meet new challenges, organizations can stay ahead of potential threats and drive sustainable growth.

Sponsor

SANS would like to thank this paper's sponsor:

hackerone