hackerone

SECURITY CONFESSIONS OF EUROPEAN CISOS:

HOW DO YOU COMPARE?

HackerOne, Europe's number one bug bounty and pentesting platform, wants to know what European CISOs' biggest security challenges are and how they really feel about working with the ethical hacking community. We asked a selection of your peers for their opinions - how do you compare?

KEY TERMS

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

Hacker-Powered Security: Any goal-oriented hacking technique that uses the external hacker community to find unknown security vulnerabilities and reduce cyber risk.

Vulnerability Disclosure Policy (VDP): A formalised method for receiving vulnerability submissions from the outside world

Bug bounty program: A way of rewarding and incentivising hackers submitting valid vulnerabilities

WHAT'S YOUR BIGGEST SECURITY CHALLENGE?

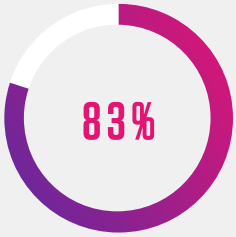
In a survey of 600 CISOs, CTOs and CIOs, **35%** said that a lack of budget and relevant skillsets were their biggest barriers to running an offensive security program.

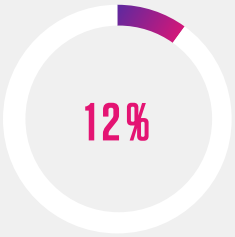
HackerOne's customer ABOUT YOU is familiar with this problem. As the company grew, the German retailer found that internal resources and the occasional pentest weren't sufficient to keep up with its security demands: network monitoring, writing security policies, running the bug bounty program, and software audits.

Internal engineers, no matter how smart, would rarely come up with the same tactics as external criminals. Starting with a managed bug bounty program, ABOUT YOU used HackerOne's triage team to help validate reports and manage communications with hackers, giving ABOUT YOU's security team time to work with developers to fix the vulnerabilities and test their solutions. Over time, the ABOUT YOU security team became more efficient, freeing up time to focus on other projects outside of vulnerability management. Read more here.

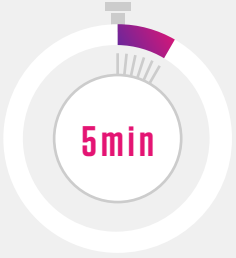
KEY STATS

83% of of European CISOs see software vulnerabilities as a significant threat to their org





Only **12%** of European CISOs believe pentests provide sufficient results to keep up with the pace of development

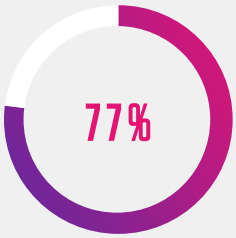


Every **5 minutes**, a hacker reports a vulnerability on HackerOne's platform

$384,793
IN SAVINGS

OVER
3 years

One organization detailed how hacker-powered pentests helped them eliminate **$156,784** in total costs and save an additional **$384,793** over 3 years by reducing internal security and application development efforts.



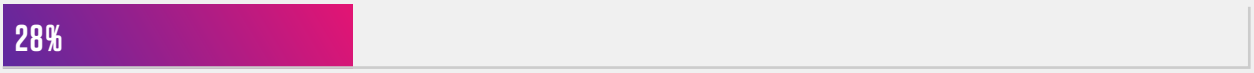
In **77%** of the cases, hackers find the first valid vulnerability in the first 24 hours

HOW MUCH DO YOU TRUST HACKERS TO SECURE YOU?

Our research shows that **57%** of European CISOs would rather accept the risk of software vulnerabilities than invite unknown hackers to find them, and **39%** say they are only comfortable accepting bug submissions from vetted hackers.

We understand embracing hackers is a daunting prospect. But the bottom line is that vulnerabilities exist, and hackers are looking for them anyway so it's better to harness the power of white hat hackers before bad actors exploit them. Some vulnerabilities can remain undiscovered for decades, as PuTTY developers found when a 20-year-old bug was uncovered last year as part of the EC funded EU-FOSSA Bug Bounty program. The vulnerability could have allowed a bad actor to crash the program, and potentially use that crash to achieve Code Execution. Working closely with the open source community of developers, the hackers working on the EU-FOSSA bug bounty programs saw 133 vulnerabilities fixed, paying out €87,990 in bounties. Read more here.

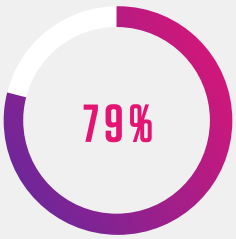
KEY STATS



28% of hackers on HackerOne's platform say they hack to do good in the world

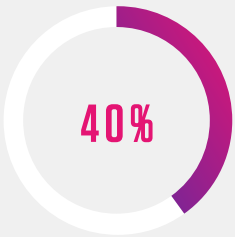
>149,000 VULNERABILITIES FIXED

Our hackers have helped fix over **149,000 vulnerabilities** for customers



79% of HackerOne's customers run private bug bounty programs

HackerOne Clear is an add-on for those who want more control over their programs to only use vetted, background checked hackers



Cleared hackers submit **40%** of all bugs resolved on HackerOne

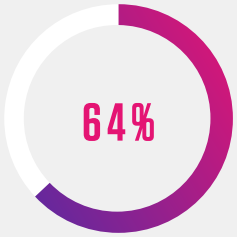
TO WHAT EXTENT DO SECURITY ISSUES POSE A RISK TO YOUR BUSINESS GROWTH?

86% of European CISOs say that software projects are stifled due to fears of inevitable security issues, with **48%** saying their organisation spends too much time fixing security issues in code. Being able to understand at an earlier stage where the security issues could cause problems and fixing them before they do will empower organisations to innovate more freely and securely.

Data from bug bounty programs can help organisations identify problems and understand how they can secure and future-proof digital assets further down the line. With bug bounty, testing is continuous, ongoing, and mirrors the SDLC.

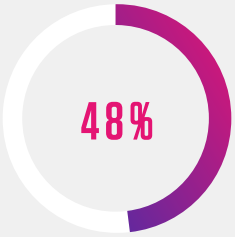
Spotify's bug bounty program helps inform the company's "Golden Paths" engineering strategy, setting out the best way to build products. This consists of a set of APIs, application frameworks and runtime environments that allow Spotify engineers to develop and deploy code securely and at scale. From the bug bounty program reports, Spotify has found that the more development adheres to a "Golden Path", the less likely there is to be a vulnerability reported. The data shows Spotify that it's possible to maintain autonomy and decentralisation in development teams while ensuring high quality. Read more here.

KEY STATS



64% of European CISOs say the pace of development in their organisation outstrips their security team's resource.

Less than half of HackerOne's Top 10 vulnerabilities overlap with the OWASP Top 10; find out more here.



A DevOps Community survey shows that 48 per cent of developers continue to believe security is important but don't have enough time to spend on it.

Of the top vulnerability types reported on HackerOne in the past year, cross-site scripting (XSS, CWE-79), remains the most common vulnerability type, although recently we're starting to see Information Disclosure (CWE-200) surpass XSS as the most common vulnerability type.

*Research Conducted by Opinion Matters on behalf of HackerOne: 31/12/2019 - 07/01/2020

Sample: 200 CISO, CTO, CIO per country (UK, France, Germany) (natural fallout on job title) working in companies employing 1000+ people