hackerone

CISO's Guide to Reducing Risk with Responsible Disclosure

Do You Have Hackers on Your Side?

Imagine someone discovers a critical security flaw impacting your customers. Would you want your team to know about it, no matter the source?

When a hacker discovers a vulnerability, they're quick to look for ways to disclose it to your security team. But if an obvious reporting channel is unavailable, hackers are faced with an undesirable choice: doing nothing, or disclosing the vulnerability publicly.

The last several years have seen the most destructive data breaches of our time. But they could have been much worse. Tens of thousands of security vulnerabilities were eliminated with the help of hackers.

"When people see a flaw in what you're doing, most people actually want to tell you," Phil Venables senior advisor and board director at Goldman Sachs said of working with hackers.

Known by some as Responsible Disclosure Policies, Vulnerability Disclosure Policies have resulted in global organisations detecting vulnerabilities impacting hundreds of millions of consumers.

In Reducing Risk with Responsible Disclosure, we will look at how top organisations including Starling, Vivy, Hyatt, Logitech and Google Play are working with hackers to protect their customers and brands.

LIVE TALK

"Having a mature and coordinated vulnerability disclosure process helps decrease the risk of an incident occurring."

OLLIE,
NCSC VULNERABILITY DISCLOSURE LEAD

READ THE BLOG POST

Easy and Safe Vulnerability Reporting

The positive power of the hacker community far exceeds the risks and the might of adversaries. To date, HackerOne has helped find and fix over 150,000 vulnerabilities for 1,600 customer programs. A quarter of valid vulnerabilities are classified as high or critical severity.

Your job is to reduce the risk of a security incident, protect your brand and assets, and ensure the security of your customers and their valuable data. Keeping those assets secure is a non-stop endeavor—but equipping your organisation with this toolbox can be prohibitively expensive. It's almost impossible to scale security with internal resources alone.

A Vulnerability Disclosure Policy (VDP), commonly referred to as a "see something, say something" approach for the internet, is an organisation's formalised method for receiving such vulnerability submissions from the outside world. The VDP instructs hackers on how to submit vulnerability reports and defines the organisation's commitment to the hacker on how reports will be handled. The practice has been outlined by the European Union Agency for Cybersecurity and in ISO 29147.

VDP PROGRAM SUCCESS

In just three years, The U.S. Department of Defense has detected more than 11,000 security vulnerabilities through their VDP program alone—winning the prestigious DoD Chief Information Officer Award earlier this month. Unlike a bug bounty program, VDPs do not offer incentives or rewards for vulnerability reports.

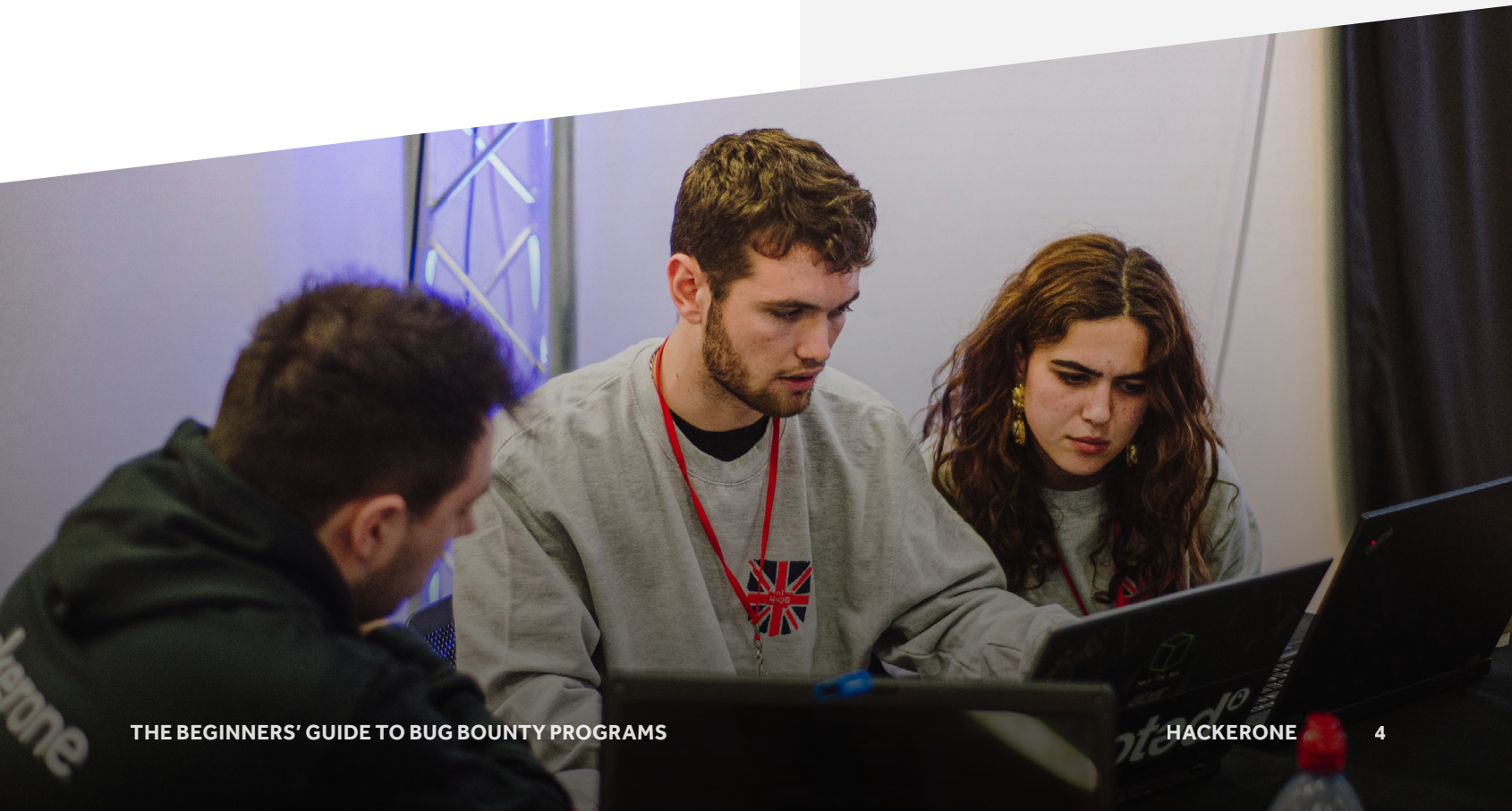
Despite the effectiveness of vulnerability disclosure policies, 93% of the world's top companies on the Forbes Global 2000 do not offer a means for contacting them to disclose a critical vulnerability.

As a result, **one in five hackers who have found a vulnerability opted not to disclose it because the company did not have a channel to receive the hacker's report.** That means at least 1 in 5 companies faces potentially critical vulnerabilities that remain unreported and unresolved. Having a VDP in place reduces the risk of a security incident or uncoordinated disclosure and places the organisation in control of what would otherwise be a chaotic workflow.

LIVE TALK

It is critical that organisations have a way for external parties to tell them about potential security vulnerabilities, leveraging their internal vulnerability management process to triage and remediate them.

SECURITY LEAD,
GLOBAL FINANCIAL SERVICES FIRM



5 Critical Components of a VDP

Every day, researchers, friendly hackers, journalists and other actors find vulnerabilities in your technology. But do they have an obvious way to alert you when they find one? A Vulnerability Disclosure Policy (VDP) gives ethical hackers clear guidelines for reporting potentially unknown and harmful security vulnerabilities. VDPs don't need to be long, nor should they require months to generate, but they should contain enough detail to help both you and the researchers improve your security.

1. **PROMISE:** Convey the mission behind the policy and explain your commitment to security, customers, and others. Include statements on why this policy was created, why it is important to have a public policy, what it is expected to accomplish.

2. **SCOPE:** Specify what is fair game, and where attention is requested or not allowed. Also state which types of vulnerabilities should be reported and which are excluded. Limitations may also be put on products or versions, or to protect data or intellectual property.

3 **"SAFE HARBOR":** Write a good faith commitment that those reporting will not be penalised. Essentially say, "we will not take legal action if..." This gives needed reassurance to those disclosing a vulnerability, so make the language inviting, non- threatening, and clear.

4. **PROCESS:** Detail how finders should submit reports and what information you would like to see. This is where you can set expectations for subsequent communications. Requesting emailed reports can lead to incomplete and unstructured information, while a secure web form like HackerOne's Response product can ensure completeness.

5. **PREFERENCES:** Set non-binding expectations for how reports will be evaluated. This section can include the duration between submission and response, confirmation of vulnerability, follow-on communications, expectation of recognition, and if or when finders have permission to publicly disclose their findings.

For more on why you need a VDP,
download the free ebook.

Responsible Disclosure is Recommended and Deployed by Governments and Industry Leaders Globally

Guidance on vulnerability disclosure has been published by numerous organisations, including the United States Department of Defense, The Dutch Government, The Singapore Government, the UK's NCSC and The European Union Agency for Cyber Security.

The International Organization for Standardization, ISO/IEC 29147:2014, has also provided guidelines for the disclosure of potential vulnerabilities in products and online services. Specifically, it details the methods a vendor should use to address issues related to vulnerability disclosure.

The reality is this: vulnerabilities are found every day by security researchers, friendly hackers, customers, academics, journalists, and tech hobbyists. Because no system is entirely free of security issues, it's important to provide an obvious way for external parties to report vulnerabilities.

LIVE TALK

"We need to move to a world where...all companies providing internet services and devices adhere to a vulnerability disclosure policy."

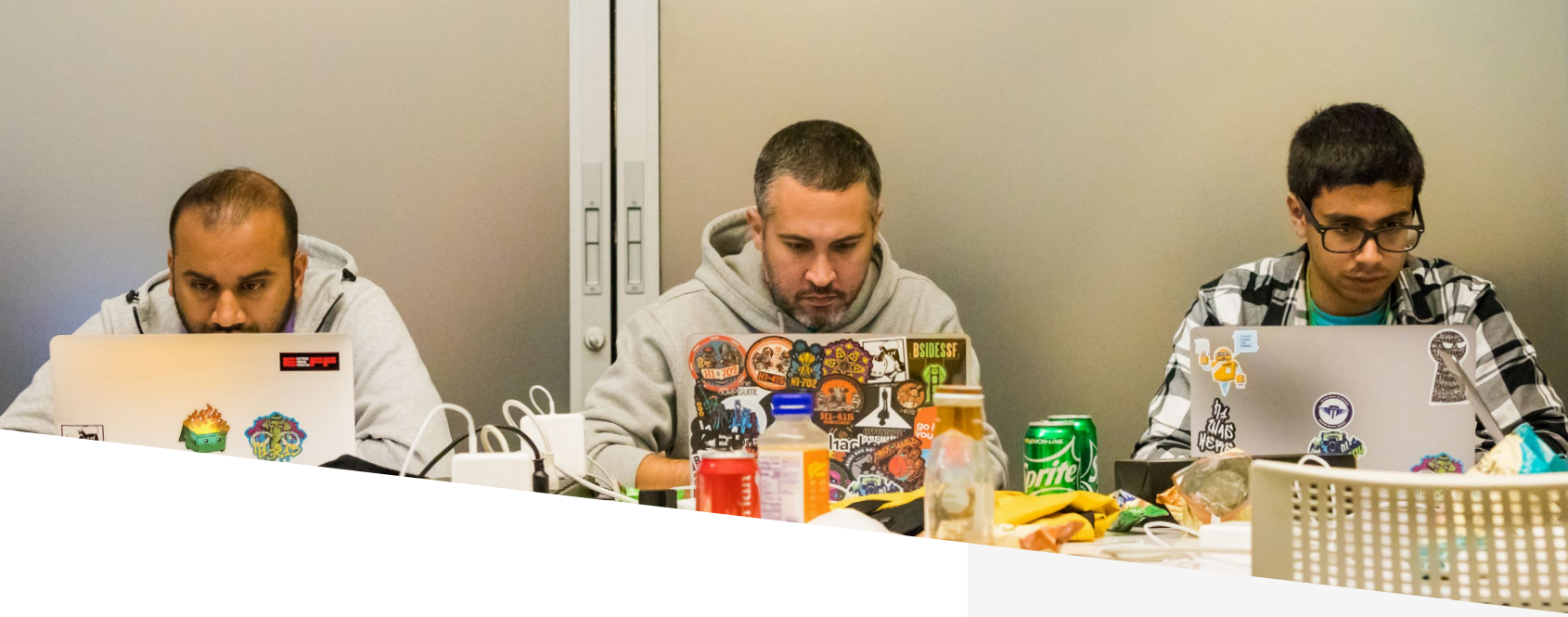
JULIAN KING,
SECURITY UNION COMMISSIONER,
EUROPEAN COMMISSION

Who are Hackers and Why Trust Them

We cannot prevent data breaches, reduce cyber crime, protect privacy or restore trust in society without pooling our defenses and asking for external help.

Youthful, hungry for knowledge, and creative. Nine out of 10 hackers are under 35, while 8 out of 10 are self-taught. More and more hackers are coming from diverse industries outside of technology, bringing myriad skillsets and perspectives to bear on their bug hunts. They're also hacking more than ever, with more than 40% spending 20-plus hours per week searching for vulnerabilities and making the internet safer for everyone.

Hackers' motivation to hack are not solely centered around monetary awards. 44% begin hacking to learn and to contribute to their career and personal growth, and nearly as many hack to have fun (49%) as much as they do it for the money (53%).. With each new company and government agency joining HackerOne every day—such as the Hyatt, GitHub, Starbucks, Starling, ABOUT YOU, European Commission, Alibaba, Goldman Sachs, Deliveroo and more—comes curiosity and a genuine desire to help the internet become more secure (9%).



Security experts may be described using a variety of titles including "hacker", "ethical hacker", "white hat", "security researcher", "bug hunter", and "finder." One title is conspicuously absent: criminal. Hackers are not criminals. Specifically, platforms like HackerOne offer no benefit to someone with criminal intent. On the contrary, reputable bug bounty platforms will record data about every hacker on the platform and only reward actions that follow the rules. For these reasons, criminals go elsewhere.

For a deep dive into the hacker community, checkout the 2020 Hacker Report.

Do you require strict finder verification capabilities? Download this datasheet to learn about HackerOne's Advanced Vetting for organisations that require strict finder verification and enhanced program controls.

600K+

TOTAL REGISTERED HACKERS

150K+

TOTAL VALID VULNERABILITIES SUBMITTED

$83M+

TOTAL BOUNTIES PAID

**As of February 2020*

See Something? Say Something with Disclosure Assistance

When a vulnerability is found, it needs to get into the right hands quickly so it can be safely resolved.

In the absence of a vulnerability disclosure policy, attempts to report security vulnerabilities often carry considerable legal risk for the hacker, so many hackers simply withhold vulnerable information or publish anonymously. When businesses do not empower hackers to disclose a vulnerability, the vulnerability puts the business and the public at risk. When hackers must report anonymously, it makes it difficult for companies to obtain key information they might need to fix the vulnerability. In both cases, it's impossible to achieve an optimal outcome that ensures security vulnerabilities are safely resolved, and it causes the internet to be less safe than it could be.

For this reason, HackerOne provides Disclosure Assistance to help friendly hackers disclose vulnerabilities to any organisation and to help create better security for the internet.

When hackers discover a vulnerability and the organisation doesn't have a vulnerability disclosure policy, **HackerOne will work with friendly hackers on a best effort basis to:**

- verify the legitimacy of a vulnerability.
- reach out to and verify the identity of an individual at the affected organisation.
- share the vulnerability with the organisation so it can be resolved.

When vulnerabilities are resolved, the internet becomes a safer place for us all. For more information on Disclosure Assistance or to report a vulnerability visit: https://hackerone.com/disclosure-assistance

Trusted Globally

From implementing the basics of a vulnerability disclosure process to supercharging your existing security via a bug bounty program, HackerOne has you covered. No matter which program or hacker-powered security choice is right for you, working with HackerOne means you work with vetted, trusted hackers. HackerOne provides several layers of control for selecting, inviting, and approving hackers based on their Reputation metrics, past program participation, specific skills, and more.

Every 5 minutes, a hacker reports a vulnerability. Every 60 seconds, a hacker partners with an organisation on HackerOne. That's more than 1,000 interactions per day towards improved security.

Do you require strict finder verification capabilities or secure VPN technology to satisfy legal requirements? Downloading the datasheets to learn about HackerOne's Advanced Vetting or VPN.

Have a question? Let us know. Learn more by visiting our website or contacting us today.

LIVE TALK

Gartner®

According to Gartner's *Emerging Technology Analysis: Bug Bounties and Crowdsourced Security Testing* report, crowdsourced security testing is "rapidly approaching critical mass".

About Us

HackerOne is the #1 hacker-powered pentest & bug bounty platform, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. With over 1,600 customer programs, including The U.S. Department of Defense, General Motors, Google, Goldman Sachs, PayPal, Hyatt, Twitter, GitHub, Nintendo, Lufthansa, Microsoft, MINDEF Singapore, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, HackerOne has helped to find over 150,000 vulnerabilities and award over $83M in bug bounties to a growing community of over 600,000 hackers. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, France and Singapore.

hackerone

Contact us to get started.