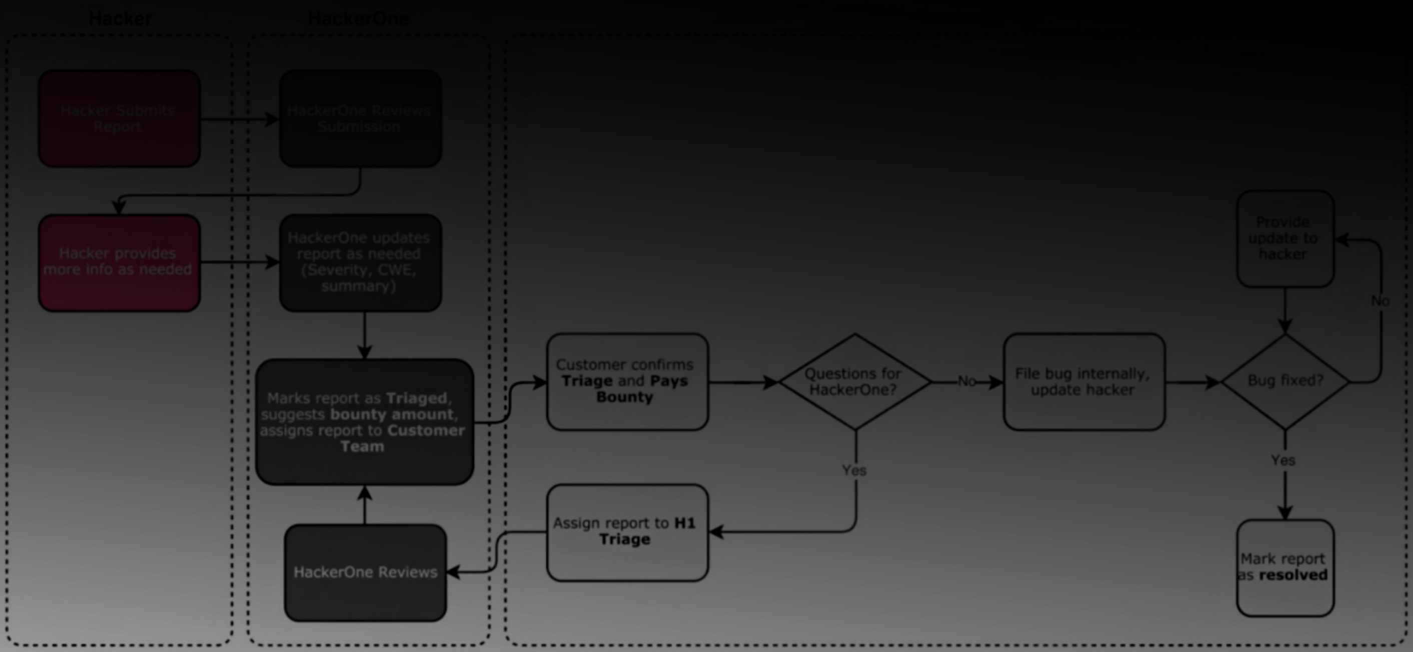
hackerone

What is a Vulnerability Disclosure Policy and Why You Need One

VDPs work and they protect assets. That's why the U.S. Department of Justice, the European Commission, and the U.S. Food & Drug Administration recommend them.


Hacker
HackerOne
Hacker Submits Report
HackerOne Reviews Submission
Hacker provides more info as needed
HackerOne updates report as needed (Severity, CWE, summary)
Marks report as Triaged, suggests bounty amount, assigns report to Customer Team
HackerOne Reviews
Customer confirms Triage and Pays Bounty
Assign report to H1 Triage
Questions for HackerOne?
No
Yes
File bug internally, update hacker
Bug fixed?
No
Yes
Provide update to hacker
Mark report as resolved

Bug bounty programs may capture the majority of headlines in hacker-powered security today, but organizations of all shapes and sizes must first open a channel for ethical hackers to alert them to potential vulnerabilities they find. It's called a vulnerability disclosure policy (VDP). It's promoted extensively from the U.S. Department of Justice to the European Commission to the U.S. Food & Drug Administration.

Why are these organizations so adamant about VDPs? Because they work and they protect assets. For example, the Department of Defense alone has received over 5,000 valid vulnerabilities through their VDP. That's thousands of potentially exploitable vulnerabilities that would have gone unfixed had they not been reported via their VDP. It's no wonder they want everyone else to have one, too.

This article will answer the simple question of what a vulnerability disclosure policy is, what's included in a good policy, which organizations have a VDP today, and which government agencies have published guidance on VDPs.

What is a Vulnerability Disclosure Policy?

A VDP is the digital equivalent of "if you see something, say something." It's intended to give anyone—ethical hackers (aka "researchers" or "finders"), anyone who stumbles across something amiss—clear guidelines for reporting potentially unknown or harmful security vulnerabilities to the proper person or team responsible.

Think of this real-life analogy: you walk past a neighbor's house and see their back door was left wide open. What would you do? You'd probably knock on their door, holler for them, or maybe even call them.

But for organizations or technology or websites, it's not that simple. You might not know how to contact them, where to even find a phone number or email address, or what to tell them. Furthermore, you wouldn't know if your email or voicemail ever made it to the correct person, or anyone at all. Or, after looking for and not finding an appropriate contact mechanism, most of us would probably give up.

VDPs are intended to remedy that situation by giving finders clear directions on how to report a potential vulnerability, and giving your internal security team an easy means with which to receive such reports. It also helps eliminate the potential business chaos should someone not know how to report a vulnerability and it winds up on social media.

Critical Elements of a Vulnerability Disclosure Policy

What's great about VDPs is they can be as simple as a few statements, and are generally just a few pages long. What's important is to include these five elements:

1. **Promise:** You state a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities.
2. **Scope:** You indicate what properties, products, and vulnerability types are covered.
3. **"Safe Harbor":** Assures that the finder reporting in good faith will not be unduly penalized.
4. **Process:** The process finders use to report vulnerabilities.
5. **Preferences:** A living document that sets expectations for preferences and priorities regarding how reports will be evaluated.

Many VDP templates and guides exist, we recommend looking at the Coordinated Vulnerability Disclosure Template published by a working group of the U.S. National Telecommunications and Information Administration.

VDP Best Practices Focus on Safe Harbor

Research shows that hackers sometimes avoid disclosing vulnerabilities due to non-existent or unclear disclosure policies. The risk of legal action is too great, they say, so the vulnerability remains open. To reassure hackers that, when acting in good faith, there will be no legal action, VDPs should include a safe harbor statement.

In March 2018, Dropbox made its VDP "a freely copyable template" for others to emulate. This is notable as Dropbox added a legal safe harbor pledge to its VDP, promising "to not initiate legal action for security research conducted pursuant to the policy, including good faith, accidental violations." HackerOne also introduced legal safe harbor language as a default for new policy pages, further solidifying it as industry standard.

What Organizations Have a VDP Today?

No organization is too small or too large to benefit from a VDP. And, many organizations are not only recommending VDPs, but are also leading the charge with their own candid insights into their own VDPs and the related benefits. However, many more companies are still leaving themselves open to unnecessary risk.

Progressive companies, regardless of industry or location, know the value of a public VDP.

The below companies are a sample of companies from the Forbes 2000 List that have a published VDP:

1. *ABB*
2. *Abbott Laboratories*
3. *Accenture*
4. *Alibaba*
5. *American Airlines Group*
6. *American Express*
7. *Apple*
8. *AT&T*
9. *Autodesk*
10. *BASF*
11. *Boston Scientific*
12. *British Sky Broadcasting*
13. *BT Group*
14. *Caterpillar*
15. *Citigroup*
16. *Comcast*
17. *Danske Bank*
18. *Deutsche Telekom*
19. *Eaton*
20. *Fiat Chrysler Automobiles*
21. *Garmin*
22. *General Electric*
23. *Honeywell International*
24. *Intel*
25. *Johnson & Johnson*
26. *Johnson Controls International*
27. *Mastercard*
28. *Medtronic*
29. *Oracle*
30. *Panasonic*
31. *Philips*
32. *PNC Financial Services*
33. *Royal Bank of Scotland*
34. *SAP*
35. *Schneider Electric*
36. *Smiths Group*
37. *Standard Chartered*
38. *Starbucks*
39. *Swisscom*
40. *Telecom Italia*
41. *Tencent Holding*
42. *Toyota Industries*
43. *Twenty-First Century Fox*
44. *Unilever*
45. *Visa*
46. *Vodafone*
47. *Walmart*
48. *Western Union*
49. *Yamaha Motors*
50. *ZTE*

Each year, HackerOne analyzes the entire Forbes Global 2000 list of the world's most valuable public companies as one benchmark for public VDP adoption. Based on the 2017 Forbes Global list, 93% of companies do not have a known VDP, compared to 94% of the 2016 list. While these numbers show marginal progress, there is obvious room for improvement. With so many organizations urging companies to adopt VDPs, along with Gartner's recent predictions that 50% of enterprises will have crowdsourced security solutions by 2022, we remain optimistic that more companies will publish VDPs soon.

But until VDP adoption increases, vulnerabilities will continue to remain unreported, and breaches will continue at an accelerated rate. Nearly 1 in 4 hackers have not reported a discovered vulnerability because the company didn't have a channel to disclose it, according to our 2018 Hacker Report.

Influence of Governing Bodies on VDPs

VDPs are seen as an invaluable tool in fighting cybercrime. Recently, government and industry organizations have begun to publish VDP how-tos, templates, standards, and related guidance on how to implement, manage, and audit these important programs.

Standardization is being applied to VDPs by various bodies, with definitions published by the U.S. Department of Justice (DoJ) and in ISO 29147. Many other organizations have published guidance or issued statements including the U.S. Food & Drug Administration which said that "manufacturers should also adopt a coordinated vulnerability disclosure policy." Still others are positioning VDPs as an effective tool to help comply with laws and regulations, specifically GDPR.

The Center for European Policy Studies, for example, recently stated that VDPs "may reduce the risk of incurring fines arising from possible personal data breaches." This suggests that, in the case of a GDPR-related breach, the absence of a VDP could be seen as worthy of penalization.

Governments and Industry Groups Continue to Promote VDPs

European Commission

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

FDA

"Manufacturers should also adopt a coordinated vulnerability disclosure policy."

NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

"Automotive industry members should consider creating their own vulnerability reporting/ disclosure policies."

NTIA
U.S. DEPARTMENT OF COMMERCE NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION

"Vulnerability disclosure has long been an open, important issue in cybersecurity."

NIST

"Coordinated Vulnerability Disclosure...is mature and ready for inclusion in the (CVD) Framework."

FEDERAL TRADE COMMISSION • UNITED STATES OF AMERICA • MCMXV

"The adoption of vulnerability disclosure policies represents a cost-effective and efficient method of identifying and addressing vulnerabilities."

CEPS

"The private sector is responsible not only for developing the best possible software, but also for responsibly handling vulnerabilities whenever they are discovered."

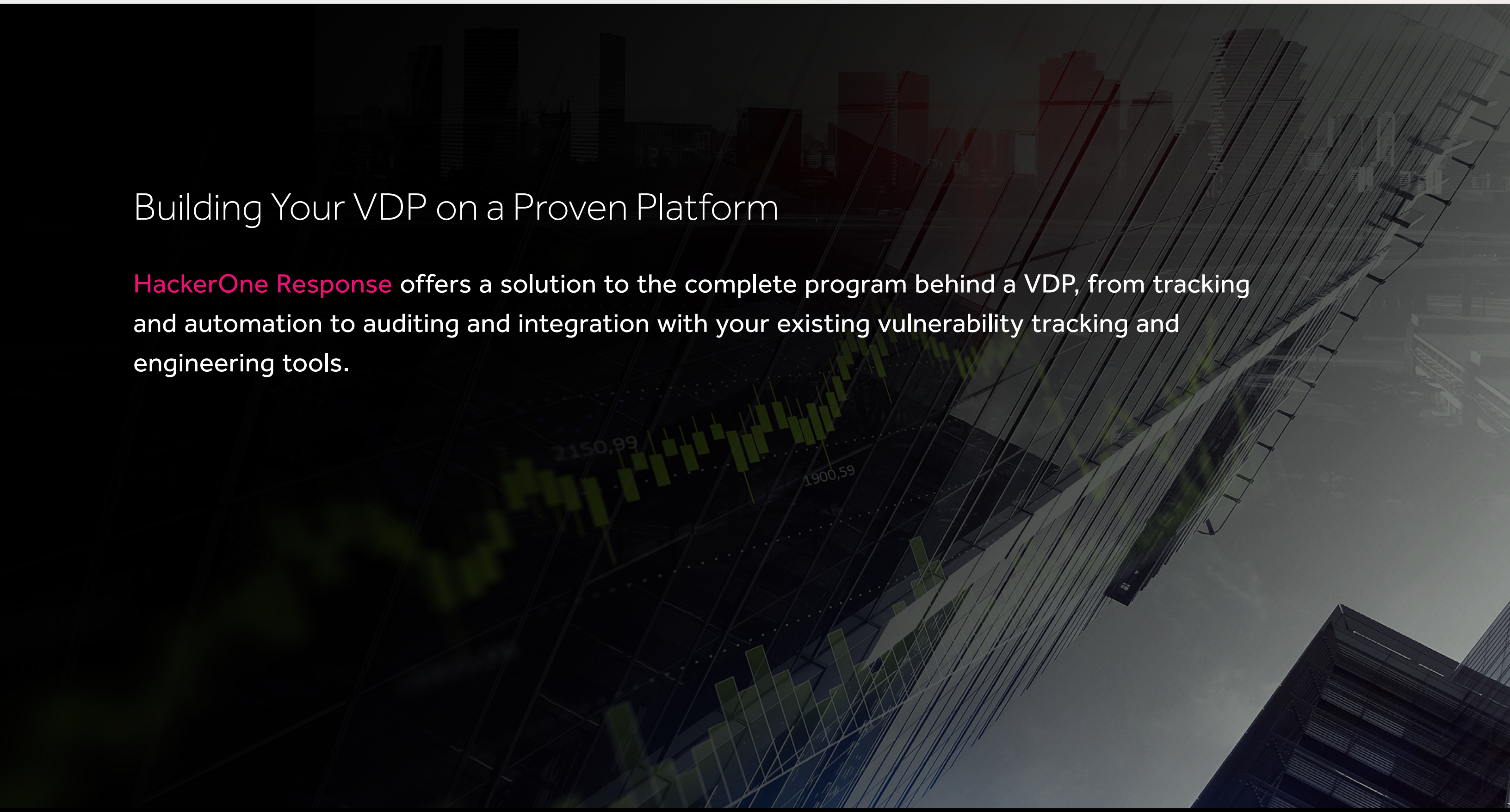
Legal Experts and Market Leaders Tout VDP Value

"To improve the security of their connected systems, every corporation should have a vulnerability disclosure policy that allows them to receive security submissions from the outside world." - Jeff Massimilla, Vice President Global Cybersecurity, GM

"All companies should consider promulgating a vulnerability disclosure policy, that is, a public invitation for white hat security researchers to report vulnerabilities found on your system." - Rod Rosenstein, Deputy Attorney General

"Companies that lack a clear vulnerability disclosure program are at increased risk should a security researcher find a vulnerability." - Megan Brown, Partner, Wiley Rein LLP

Read what others had to say in Voices of Vulnerability Disclosure.



Building Your VDP on a Proven Platform

HackerOne Response offers a solution to the complete program behind a VDP, from tracking and automation to auditing and integration with your existing vulnerability tracking and engineering tools.