7 steps for implementing a Vulnerability Disclosure Program

bugcrowd

Cybersecurity vulnerabilities are present everywhere and can lead to serious legal, financial, and reputational damage for companies.

The vulnerabilities that permeate complex systems can impact both enterprise and personal data. If these vulnerabilities are exploited, the real-world consequences can be significant.

Thus, it goes without saying that cybersecurity is a major concern not only for individuals but also organizations. We are starting to see unprecedented change in the industry as well—change for the better.

With policies and standards such as the NIST Cybersecurity Framework in place, it's now incumbent on organizations to ensure they are prepared to receive vulnerability data from external parties. Such efforts are already becoming an adhered-to standard for major private organizations.

A Vulnerability Disclosure Program (VDP) is a vital part of how companies are managing the risks that vulnerabilities can pose. The recent momentum behind these types of programs shows that corporations and government agencies alike are committed to taking vulnerabilities seriously. Furthermore, they are making the disclosure of their vulnerability efforts more transparent.

But setting up a VDP is not always intuitive, and understanding what goes into the process can be even more difficult. Knowing what questions to ask before jumping in can set you up for success. This guide will go over seven key steps in implementing a VDP.

Frequently asked questions about VDPs

Before we dive into the seven key steps, let's answer a few FAQs about VDPs.

1 What types of submissions go through VDPs?

87% of organizations report receiving at least one critical vulnerability through their VDPs (take into consideration that in 2024, the average cost of a breach was estimated to be $4.84M). VDPs are a great way to get submissions of all severity levels.

2 Are VDPs necessary to meet certain compliance requirements?

Having a VDP is quickly becoming industry standard and is, in fact, no longer optional for certain organizations and industries. There is an increasingly popular belief throughout the cybersecurity industry that VDPs are a must for compliance and that they establish a baseline for security best practices.

Here are three examples.

Binding Operational Directive 20-01

The Binding Operational Directive 20-01 issued by CISA requires all 100+ Federal Civilian Executive Branch agencies to develop and implement a VDP. This means that vulnerability disclosure policies are now a federal mandate. Since this requirement went into place, these agencies have had massive success with their VDPs.

U.S. Securities and Exchange Commission (SEC) ruling regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

In July 2023, the SEC adopted new rules stipulated in a guide titled "Cybersecurity Risk Management, Governance, and Incident Disclosure." The ruling requires organizations to disclose material cyber incidents within four days of determining the criticality of an incident. To be in a position to responsibly comply, organizations must have in place the processes necessary to meet the four-day requirement.

One thing organizations can do to facilitate these processes is to provide a clear, unambiguous method for the public at large to report vulnerabilities under a safe harbor, aka, a VDP Learn more about these rules here.

Cyber Resilience Act (CRA)

The EU's CRA (for which Bugcrowd was an advisor) seeks to ensure that "hardware and software products (have) fewer vulnerabilities, and manufacturers take security seriously throughout a product's life cycle." Specifically, the CRA will regulate all products that depend on remote data processing (which is nearly everything, these days).

Under the CRA, manufacturers of "critical" products will be required to carry out security assessments across a product's life cycle and implement various vulnerability handling procedures. These include adopting a policy for coordinated vulnerability disclosure, creating a software bill of materials (SBOM), and remediating flaws without delay.

3 What is the difference between a VDP and a bug bounty program?

VDPs and bug bounty programs are now critical tools to have in your security toolbox, but which tool should you use for which job?

Let's compare:

VDP

A VDP is a secure, publicly available channel for anyone to submit security vulnerabilities to organizations. Such submissions help organizations mitigate risk by enabling the disclosure and remediation of vulnerabilities before they are exploited by bad actors. In contrast to bug bounties, VDP submissions are not incentivized by cash rewards. Publishing a vulnerability report after it has been fixed is another common attribute of VDPs. Such reports give hackers the opportunity to share knowledge and enhance their own reputations in the process.

PRIVATE BUG BOUNTIES

Private bug bounties, which are often run during a point in time and have a use case similar to that of penetration tests, are often narrower in scope than their public counterparts (e.g., more tightly focused on specific targets). Hackers are incentivized by cash bounties (aka "pay for results"). Private bug bounties limit participation to handpicked hackers, which allows for targeted skill matching, along with background checks, geographic selection, and so on.

PUBLIC BUG BOUNTY

A public bug bounty allows anyone to participate. It's similar to a VDP but with the addition of cash and other rewards to incentivize proactive testing. Another trait of bug bounty is that testing efforts are directed by organizations themselves to specific areas where security is deemed most critical.

You can learn more about how to determine which type of engagement is right for you here.

Seven steps to a successful VDP

STEP 1

Determine your business goals

One very important thing to consider before creating a VDP is your goal. What do you want to get out of a VDP program? How will your program help move the needle?

1	**Reduce risk**	
2	**Improve security ROI**	
3	**Demonstrate security maturity**	
4	**Improve security transparency and customer confidence**	
5	**Establish and promote more positive cooperation between internal and external parties**	
6	**Achieve compliance requirements**	

Before moving forward with a VDP, it's important to agree on a set of goals and communicate them across your company. This way, you'll know what success looks like, and you'll be able to report on it.

STEP 2

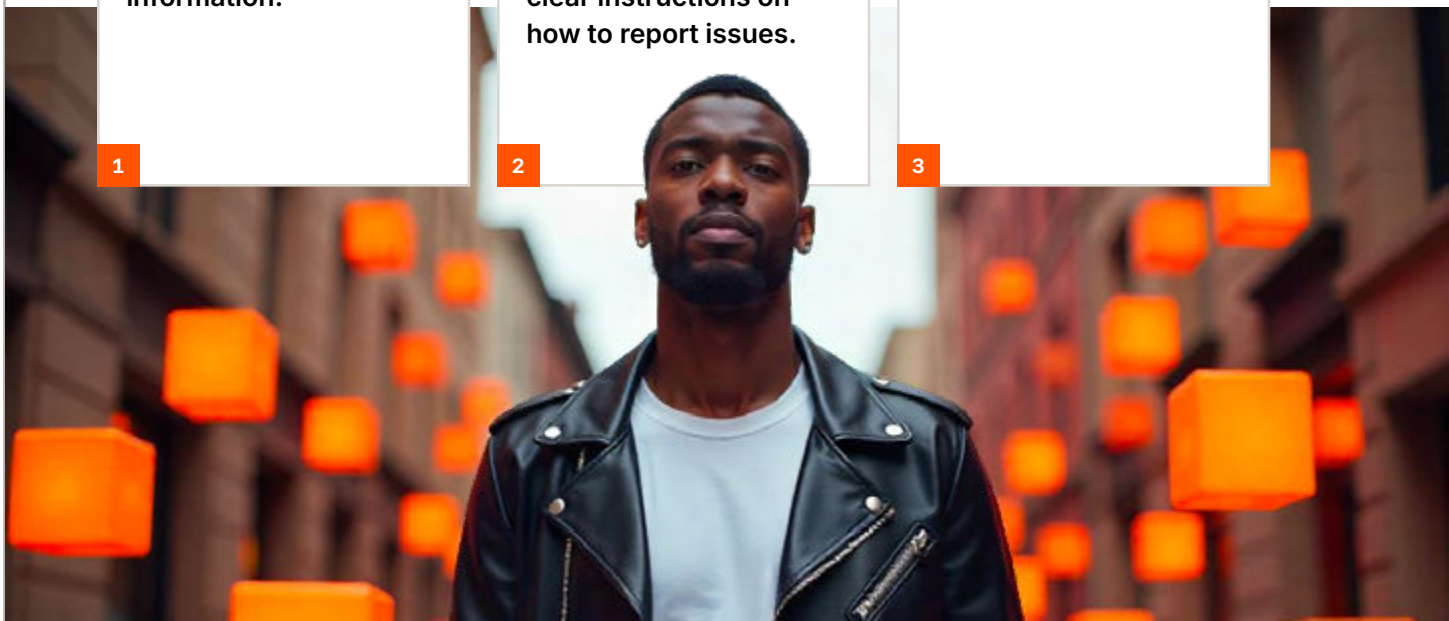
Look for three primary components of your VDP

A VDP is the initial first step to protecting your company from an attack or premature vulnerability release to the public. A VDP is quickly becoming an expected or even a required practice, with positive pressure on the model from legislature, industry peers, and even consumers.

A VDP is a process by which an organization can receive cybersecurity vulnerability reports from any external individual, whether it's a customer, a private security researcher or hacker, or a governmental body, via a dedicated channel. Every VDP is different and should be tailored to the specific threat profile, regulation requirements, and assets pertinent to your enterprise. However, all VDPs share three primary components:

VDPs share three primary components

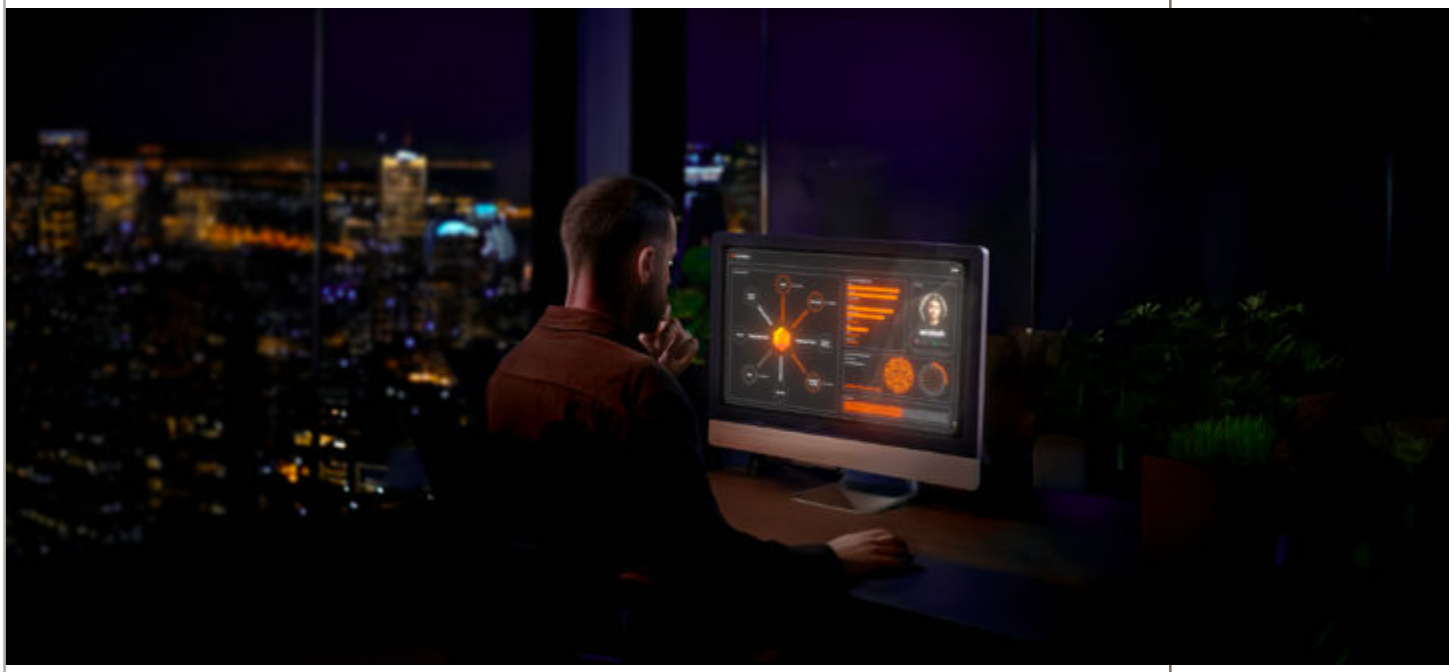
1. **A website or other communication channel through which an organization or its vendors can receive vulnerability information.**
2. **An external-facing policy that sets out clear expectations, establishes safe harbor for hackers operating in good faith, and provides clear instructions on how to report issues.**
3. **A back-end process flow that dictates how a given vulnerability will be validated and, if necessary, remediated.**



STEP 3

Select a managed VDP platform

Managed VDPs help alleviate the burden of the time and effort required to construct and run an effective disclosure program.



Look for a platform that:

- **Designs and manages email—and website—embedded submission forms**
- **Validates, categorizes, and prioritizes vulnerability submissions**
- **Integrates with your organization's software development tools for faster remediation**
- **Communicates with hackers**
- **Lists your program on its site to bring more attention to it and increase the likelihood of additional activity and submission volumes**

STEP 4

Choose what assets are in the scope of your VDP

Before moving forward with a VDP, it's important to understand what company assets you have at hand. After all, you can't secure what you don't know exists. One organization can have hundreds of subsidiaries, which brings with them thousands of web domains, subdomains, products, APIs, etc.

This is where an external attack surface management tool like Bugcrowd EASM provides huge value in discovering the full breadth of external risk exposure.

It's important to note that a VDP is the functional equivalent of a "neighborhood watch" for your company assets. You invite people who can identify unknown issues to say something if they see something. For this reason, scoping isn't as critical to a VDP as it is to a crowdsourced security program with cash incentives, like a bug bounty program.

The decision to go open scope can be influenced by the sensitivity of information stored, the ability to segment components, business and security priorities, or security or contractual limitations that are already in place.

STEP 5

Determine how you're going to receive incoming vulnerabilities

One of the main components of a VDP is having a way to receive vulnerabilities from external parties.

Having a clear and visible channel to receive bugs is the only way to mitigate premature public disclosure, which can cause negative press and/or force you to scramble to remediate a vulnerability. 58% of hackers won't report a vulnerability if the owner of that vulnerability doesn't provide a clear way for doing so.

Traditionally, the only way companies were able to receive vulnerability information was through email. Thankfully, the industry has evolved immensely.

There are now several different ways to receive vulnerabilities:

Email

Embedded submission forms

Managed VDP platforms

When thinking about how you will receive vulnerabilities, you should also consider how those vulnerabilities will be communicated internally. Emails and PDFs are simply not an effective method, given your primary audience will be your developers. Think about using tools like Slack, Jira, Clubhouse, or GitHub, as well as standardized workflows, structures, and an intuitive course of real-time communication.

STEP 6

Decide how you're going to manage incoming vulnerabilities

The process of managing vulnerability reports can be painfully time-consuming. Organizations do not have the time or resources to triage and validate incoming vulnerability findings from outside hackers. It is vital to designate a key stakeholder, team, or partner to conduct technical reviews and escalate any valid vulnerability submissions. They must also facilitate hacker communications, which are crucial for detailed reports, deeper context, and higher engagement.

Hackers put a lot of time and effort into their submissions. For this reason, Bugcrowd believes that every submission deserves a reviewer's full attention and a quick response. If there isn't a quick response, the commitment made by the program's policy will not be met, and strong, skilled hackers will lose interest.

The Bugcrowd Platform provides engineered software and services for crowdsourced security, escalating high-priority issues within hours and completing triage within one business day, on average.

Our response time is unsurpassed—our average time to first response for all submissions is well under the 24-hour SLA we set for critical vulnerabilities.

STEP 7

Learn and improve

VDPs are not just a box to be checked—they are an evolving security tool that requires regular insights to continuously improve. It's important to regularly check in with your managed VDP provider to troubleshoot processes and find areas to grow.

Bugcrowd's fully managed VDP provides reporting with data based on thousands of past customer experiences, helping customers decide their next step and evolve their programs.

Learn more about VDPs

With a managed VDP, organizations create a channel for security feedback. This information can help them to quickly identify vulnerabilities and reduce risk in an efficient and cost-effective manner.

VDPs require the right combination of policy, resources, and support to be successful. It is important to ask the right questions before implementing your VDP so that you are set up for success.

GUIDE
Ultimate Guide to Vulnerability Disclosure

DATA SHEET
Vulnerability Disclosure Programs

GUIDE
10 Essentials to Look for in a Crowdsourced Security Platform