hackerone

UNLOCKING HACKER INSIGHTS:

VULNERABILITY DISCLOSURE PROGRAM BEST PRACTICES

Take The First Step to Embracing Hacker-Powered Security.

"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

WHAT IS A VULNERABILITY DISCLOSURE PROGRAM?

Vulnerability disclosure programs (VDPs) — also known as coordinated or responsible disclosure — are are frameworks for agreement that encourage and enable security researchers to report security issues, vulnerabilities, or bugs they discover. It's the digital equivalent of "if you see something, say something."

Think about it like this. If you walked past your neighbor's house and noticed their door was left wide open, what would you do? Most likely, you'd check to see if they were home so you could let them know.

Ideally, things would be just as easy when it comes to reporting vulnerabilities. Unfortunately, it isn't. Based on the letter of the law — as laid down by the Computer Fraud and Abuse Act — any unauthorized use of a digital service that falls outside its terms of service is automatically assumed to be malicious. Simply, the law doesn't recognize the possibility of 'good faith' security research.

That's a problem because it makes life hard for security researchers who want to report any issues they find. Countless vulnerabilities have gone unreported because the 'finder' was worried they would face legal action.

And that's not the only reason vulnerabilities go unreported. Many organizations don't publish a clear route to report vulnerabilities, making it hard for researchers to know where (or how) to submit them.

However, with a VDP that sets out clear guidelines for reporting vulnerabilities, organizations enjoy the benefits of collaborating with security researchers. By implementing a VDP, your organization:

- Provides a framework for engaging with the security researcher community.
- Helps to align its cybersecurity program with industry best practices.
- Demonstrates its commitment to cybersecurity.
- Allows researchers to report vulnerabilities through a safe channel without fear of prosecution.
- Improves its ability to find and fix vulnerabilities.

"We've always approached security with a diverse set of tools in our toolbox," said Jeff Massimilla, Vice President Global Cybersecurity at General Motors. "Leveraging HackerOne's relationship with the research community and seeing firsthand the results they provide has been extremely encouraging. Hackers have become an essential part of our security ecosystem."

THE AGE OF THE VDP

VDPs are a best practice in the tech industry thanks to companies like Google, Facebook, and Microsoft. These companies augment their cybersecurity programs with the support of hackers around the world.

Many cybersecurity frameworks now include VDPs as a best practice. In the US, VDPs were first added to the NIST Cybersecurity Framework (CSF) as a recommendation for critical infrastructure organizations. More recently, NIST SP 800-53 and 53B made VDPs a recommended control for all US government agencies.

VDPs are also recommended by the US DoD, DoJ, FDA, National Highway Traffic Safety Administration, National Telecommunications and Information Administration, and FTC. Internationally, they are listed as a best practice under ISO/IEC 29147.

In 2020, The Cybersecurity and Infrastructure Security Agency (CISA) went a step further by issuing Binding Operational Directive (BOD) 20-01, which requires all federal civilian agencies to develop and publish a VDP encompassing all Internet-accessible systems. And it's not just US agencies that believe VDPs are the future:

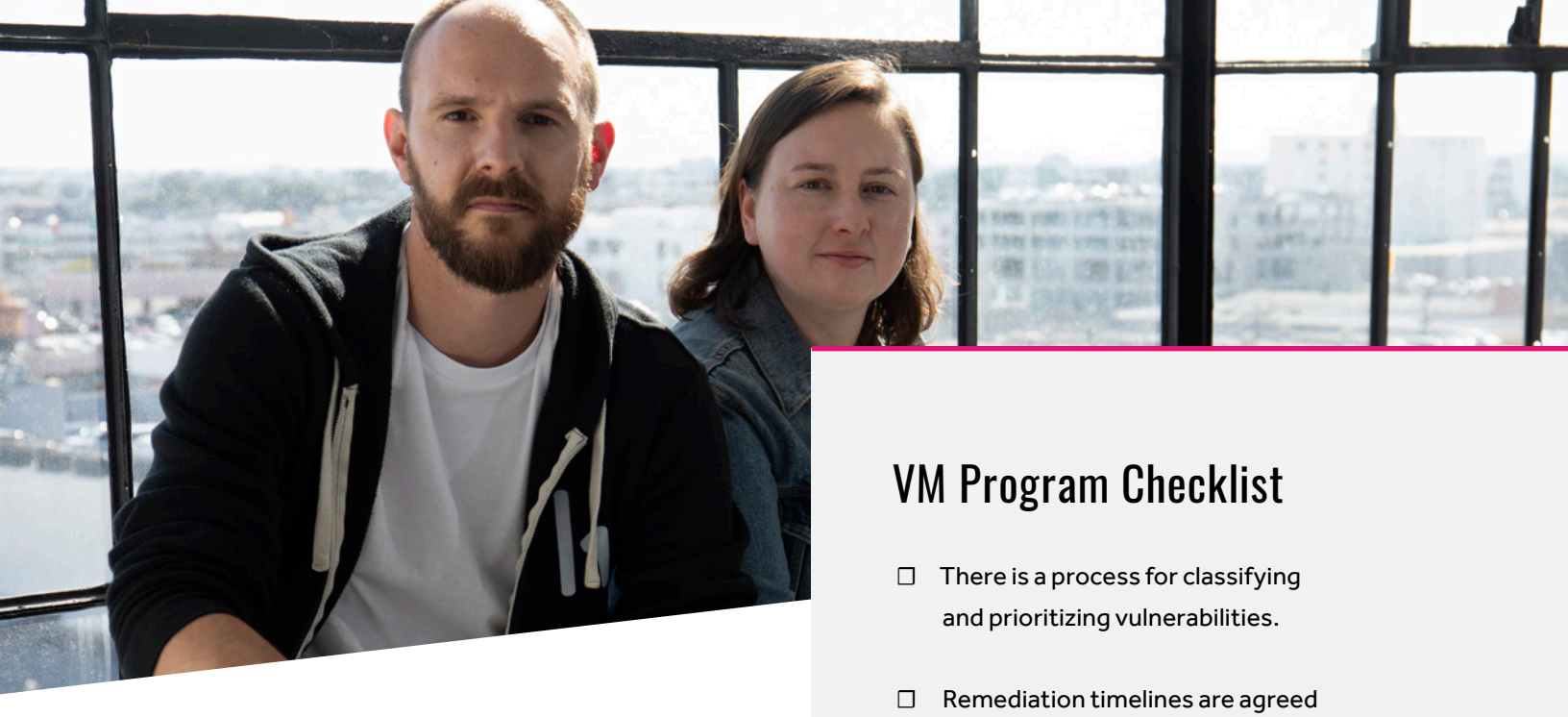
- The UK Internet of Things Code of Practice recommends VDPs for all IoT manufacturers and stakeholders.
- 'Cyber Security for Consumer Internet of Things: Baseline Requirements' is a standard for the EU, requiring all IoT manufacturers to publish a public VDP.
- The Australian Government Information Security Manual (ISM) recommends VDPs for all organizations.

Based on current trends, expect to see more regulatory bodies embrace VDPs within the next few years. Industries that are heavily targeted by cyber threats — including healthcare, eCommerce, financial services, SaaS, and enterprise technology — all have a huge amount to gain from responsible disclosure.

Security researchers will find vulnerabilities no matter what you do. Would you prefer to receive those vulnerabilities through a safe channel... or have them published to the world? Or, even worse, for researchers to 'sit on' vulnerabilities indefinitely because they are afraid of legal action?

Consider this: when HackerOne surveyed the largest community of hackers in the world, 50% said they have chosen *not* to disclose a vulnerability they found. Of those, 27% said this was because there was no channel to disclose it through, and another 27% said it was because the company had previously been unresponsive.

Simply, not having a channel for vulnerability disclosure is dangerous — and it's a risk you don't need to take.



VULNERABILITY MANAGEMENT

The entire foundation of a VDP is based on your organization's ability to resolve vulnerabilities. As such, the first priority is to ensure you have consistent and robust vulnerability management (VM) processes in place.

Strong VM programs use issue tracking tools (e.g., Jira, Assembla) to track vulnerabilities from discovery to resolution, regardless of the discovery source. This ensures vulnerabilities are not 'lost,' and teams can report on the number and severity of issues found, fixed, and retested. Note the importance of retesting — if your organization doesn't retest after each fix, there's no guarantee a vulnerability has been resolved.

Having a formal process in place to track, fix, and retest vulnerabilities is essential. Before publishing a VDP, your organization must ensure that its VM processes are robust, effective, and able to cope with a new stream of security researcher-reported vulnerabilities.

VM Program Checklist

- ☐ There is a process for classifying and prioritizing vulnerabilities.
- ☐ Remediation timelines are agreed based on severity and prioritization.
- ☐ Asset management processes ensure vulnerabilities are assigned an 'owner.'
- ☐ Vulnerabilities are tracked from report through to fix and retest.

Once you have a robust VM program in place, a VDP provides a valuable extra source of vulnerability reports. Traditional discovery methods such as vulnerability scanners and static/dynamic application security testing (SAST/DAST) are crucial, but they can't uncover complex multi-stage or 'chained' vulnerabilities.

By contrast, security researchers have the expertise, persistence, and creativity to uncover these critical vulnerabilities that are at high risk of being exploited in the real world. Having a VDP in place opens the door to these inputs and helps your organization manage the cyber risk posed by unknown vulnerabilities.

VDP vs. Bug Bounty

The most common misunderstanding about VDPs is how they differ from bug bounty programs. In practice, the two have clear differences.

A VDP offers third parties (security researchers, customers, partners, etc.) a safe channel to report vulnerabilities should they find one. A VDP does not offer monetary incentives, known as bounties, for individuals to report vulnerabilities.

On the other hand, a bug bounty program directly incentivizes security researchers to look for vulnerabilities in specific assets by offering payment in return for verified vulnerabilities within a carefully outlined scope.

The difference comes down to reactive vs. proactive security testing. While a VDP opens the door to security researchers, it doesn't (usually) provide a clear incentive to attract their expertise. As a result, any vulnerabilities your organization receives via its VDP are at the discretion of third parties (security researchers, customers, partners, etc.). On the other hand, a bug bounty program directly incentivizes submissions, which helps to attract the most qualified and experienced security researchers to test your organization's assets continuously.

You can think of a VDP as being a precursor to bug bounty. Often, organizations implement a VDP and, after seeing the security benefits it provides, launch a formal bug bounty program. However, even if your organization never 'takes the plunge' into bug bounty, a VDP is still a huge step forward for your security.

INTERNAL REQUIREMENTS FOR A VDP

A VDP is more than just a policy. Your organization doesn't just need to be willing to accept vulnerability reports. It must be ready to resolve vulnerability reports. This section will cover the internal capabilities your organization should develop before publishing its VDP.

ROLES AND RESPONSIBILITIES

One aspect of VDPs that catches many organizations off-guard is the number of stakeholders who need to be involved. Handling vulnerabilities reported by members of the public requires input from individuals and teams throughout the organization — and you must secure their buy-in before launching your VDP.

At a minimum, make sure to include:

Security

Your security team will need to classify and prioritize vulnerabilities and advise engineers on patching and remediation. Having buy-in and input from your security team is paramount to the success of your VDP.

Since your VDP, by nature, identifies vulnerabilities that were missed by existing security processes, you may find that some members of your security team are defensive or resistant. To minimize this, make it clear that:

- Vulnerabilities reported by security researchers aren't a failure on the part of your security team.
- This is an added-value measure to reduce cyber risk — NOT an effort to 'show up' security personnel.

Engineering

Your engineers are ultimately responsible for fixing reported vulnerabilities. However, nobody likes unexpected work. To keep engineers on your side, take these steps:

- Involve engineers from the outset so they can assign resources to handle incoming vulnerabilities.
- Help engineering leaders see the value of a VDP — both to their teams and the organization.
- Find a way to integrate reported vulnerabilities with existing engineering workflows.

Legal

Most legal teams are naturally wary when introduced to the idea of a VDP. Explain the purpose, value, and — depending on your industry — compliance or regulatory need for a VDP. Make it clear that a VDP creates the groundwork to enable safe and conscious dialogue with security researchers. It can also help to explain how a VDP works and what security benefits it provides for your organization.

Ultimately, your legal team will need to approve your VDP before you can publish it. To avoid friction and delays, invite your legal team to review the VDP and 'rules of engagement' early in the process and enlist their help to ensure your policy adequately protects your organization's interests.

Public Relations

Your PR or Communications team needs to know what your VDP is, why it exists, what the benefits are, and how to communicate about it to customers, partners, and other stakeholders. Help them prepare for questions that could arise once your program is launched. For instance:

- What is a vulnerability disclosure program?
- Why does your organization have one?
- Who is allowed to participate?
- What are participants allowed (and not allowed) to do?
- Why is this an important security initiative?

Because of the nature of a VDP, there may be public conversations about it — for instance, security researchers discussing vulnerabilities, celebrating 'wins,' or (if allowed) publishing write-ups of how they found a vulnerability. Help your PR team see that all of this is OK and that raising awareness of your policy will ultimately yield better results in the form of more reported vulnerabilities.

VDP BEST PRACTICES

As with any business initiative, there are some best practices you should follow when developing your VDP. However, before you start work on the policy itself, there are two essential questions to ask.

What are the Business Objectives?

Like all aspects of cybersecurity, your VDP is a business initiative. It's designed to reduce cyber risk in a meaningful and measurable way. For that to be possible, you should set specific business objectives that will govern decision-making and help you to track the effectiveness of your VDP over time.

Common business objectives include:

- Minimize cyber risk from unknown vulnerabilities.
- Minimize the risk of 'full disclosure.'
- Demonstrate security maturity to stakeholders, shareholders, partners, customers, suppliers, etc.
- Promote cooperation with the hacker/security researcher community.

Where possible, develop metrics around these objectives to ensure your policy remains effective and that any issues are identified and resolved promptly.

Where Does Your Risk Lie?

When you first launch your organization's VDP, you may choose a low-priority asset to be the 'guinea pig' — and there is some sense to this. However, once your VDP is in place and proven to be effective, you should choose further assets based on their significance to your organization.

Simply, rather than asking "which assets pose the lowest effort?" instead, ask, "where can responsible disclosure most benefit our organization?"

Since most organizations base their security operations on controlling cyber risk, it's likely that you already know which assets are most critical. While it may require more resources to include these assets in the scope of your VDP, by doing so, you will maximize the security value of your policy.

5 Critical Components of a VDP

As important as it is to get your VDP right, it doesn't have to be complicated. An effective VDP is often only a few pages long and needs just five components:

1. **Promise.** You state a clear commitment to customers — and other stakeholders who could be affected by a vulnerability in one of your assets — that your organization takes security seriously.

2. **Scope.** You specify which assets, systems, products, and vulnerability types are covered by the VDP. This scope should be flexible and expand over time — you may only include your most important assets initially, but over time you should aim to cover your entire Internet-facing environment.

3. **Safe Harbor.** You provide legally binding assurance that security researchers will not be penalized for searching for and reporting vulnerabilities in good faith.

4. **Process.** You provide a clear process that security researchers can use to report vulnerabilities.

5. **Preferences.** You set (non-binding) expectations on how long it will take your organization to acknowledge, assess, communicate, and resolve reported vulnerabilities.

Make sure your policy includes all of these — and satisfies your legal team — and you can't go too far wrong.

Common VSP Mistakes

Simple mistakes can seriously harm the success of your VDP. Here are some of the most common culprits:

1. **Not responding to security researchers.** If they feel ignored, security researchers may resort to public disclosure.

2. **Being too restrictive.** Limiting scope or testing methods too tightly prevents your organization from gaining the maximum benefit from its VDP.

3. **Expanding too quickly.** Conversely, you don't want to overwhelm internal resources before your new processes are proven. Best practice is to start small and expand your policy over time.

4. **Writing in 'legalese.'** Your VDP has to satisfy the organization's legal team, but the audience is security researchers — so prioritize language that is clear and easy to understand.

5. **Not fixing vulnerabilities.** If you don't fix vulnerabilities promptly, you open your organization to unnecessary cyber risk and discourage security researchers from contributing to your program.

Other Considerations

Scope Should Expand Over Time

For most organizations, the easiest way to launch a VDP is by initially restricting the scope to a small number of assets. This ensures your internal resources won't be swamped with reports right away and gives you a chance to 'iron out' any issues in your processes in relatively low-stress conditions.

However, VDPs are not meant to be static. For instance, CISA BOD 20-01 requires that 'At least one internet-accessible production system or service must be in scope at the time of publication,' and that one additional asset must be added to the scope at least every 90 days after that. Ultimately, the objective is for agencies to include all Internet-accessible assets in the scope of their VDP.

Adding assets over time gives agencies the chance to adapt to — and optimize — their processes, enabling them to get the maximum benefit from their VDP without overwhelming internal resources.

This approach, which is a regulatory requirement for US Government agencies, is a good blueprint for any organization considering launching a VDP.

Clearly Highlight Disclosure Terms

Before launching your organization's VDP, you must decide whether to allow security researchers to publish the details of any vulnerabilities they discover once resolved. There are three ways to approach this:

1. **Non-Disclosure.** Researchers are never allowed to publish details of vulnerabilities they discover in your systems.

2. **Coordinated Disclosure.** Your organization will coordinate with researchers on a case-by-case basis to determine if and when they can publish details of discovered vulnerabilities.

3. **Timed Disclosure.** Researchers can publish details of discovered vulnerabilities after a set time.

Keep in mind that one prominent reason why security researchers hunt for vulnerabilities in your digital assets is to raise their profile — and publishing reports is one way for them to do this. As a result, you may find that limiting or disallowing reporting of discovered vulnerabilities leads to lower engagement in your VDP.

Policy Templates

Numerous guides and templates have been published to help organizations get a VDP up and running quickly. Good places to start include General Motors, Adobe, and Vend.

Other examples include:

- The US Department of Defense VDP, which as of January 2021, has uncovered more than 26,617 vulnerabilities.
- The Coordinated Vulnerability Disclosure Template published by a working group of the U.S. National Telecommunications and Information Administration.
- Dropbox's public VDP, which it has made a freely copyable template.

WHAT DOES SUCCESS LOOK LIKE?

As with all aspects of cybersecurity, the success of a VDP depends on how effectively it reduces cyber risk for your organization. More specifically, you can think of success as:

$$\frac{\text{Cyber Risk Reduction}}{\text{Resource Cost}}$$

In effect, we're talking about security ROI. While it's not possible to perfectly understand the ROI of risk reduction, a set of well-planned and consistently monitored metrics gives you a solid foundation to work from.

To track the security value of your VDP, establish your metrics for success. These can include:

- Number of valid vulnerabilities reported
- Number of security researchers contributing to your program
- The rate of false positives
- Average time to first response
- Average time to triage
- Average time to resolution

By measuring and tracking these metrics — and others like them — over time, your organization can optimize its processes to maximize security ROI.

But what about resource costs? In effect, the 'resourcing success' of your VDP depends on your ability to funnel reported vulnerabilities into existing engineering and security workflows. If you can achieve this in a reasonably seamless manner, the resource cost of reported vulnerabilities should be minimal.

Of course, you should expect your VDP to require an upfront investment of time and resources as all internal stakeholders accustom themselves to their new roles. Over time, however, you should aim to absorb these roles into 'business as usual,' maximizing your policy's security ROI.

Go Beyond the Bug

But you shouldn't stop there. To get the most from your policy, establish metrics to help you understand the vulnerabilities being reported. For instance:

- Reported vulnerabilities by category
- Reported vulnerabilities by asset type
- Reported vulnerabilities by severity

Over time, look for patterns in these metrics that help you understand the types of vulnerabilities being found in your assets. Any trends that arise in these metrics will enable you to implement controls within the Secure Development Lifecycle (SDLC) that prevent similar vulnerabilities from being introduced into future code.

For instance, if security researchers consistently report SQL Injection vulnerabilities over time, you might provide additional training for your engineers to help them avoid introducing similar vulnerabilities in the future. Alternatively, your engineering team might decide to build automated security scanning into the development pipeline, which would help to prevent simple vulnerabilities from being pushed into live builds.

Over time, this will enable you to eliminate entire categories of vulnerabilities, drastically reducing cyber risk.

VDP Reporting

Reporting is an essential component of any VDP. Depending on your industry, your organization may be required to report certain metrics periodically — but even if you aren't, establishing a formal reporting program is an excellent way to ensure your policy remains productive over time.

From a regulatory perspective, CISA BOD 20-1 requires federal agencies to report a formal set of metrics via the CyberScope portal within 270 days of publishing their VDP.

For organizations aiming to comply with NIST 800-53, NIST CSF, ISO 29147, or another prominent framework, simply prepare to review key metrics periodically and modify your policy page as appropriate.

hackerone

HackerOne pioneered responsible disclosure. We've helped thousands of organizations establish and manage VDPs, including:

Our VDP structure is based on the recommended practices outlined in NIST CSF. Now, HackerOne has become the first hacker-powered security vendor to receive FedRAMP authorization.

To learn more, visit
https://www.hackerone.com/product/response.