
hackerone

# VULNERABILITY DISCLOSURE:

## CONSIDERATIONS, RISKS, AND COSTS


**Vulnerability Disclosure Programs** (VDPs) are, at the most basic level, mechanisms for security researchers to report vulnerabilities they find to an organization. VDPs are not only a security best practice but they are also becoming increasingly prevalent in security frameworks like NIST SP 800-53 Rev. 5 and mandates like the Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 20-01, which requires that all United States civilian agencies develop and publish a vulnerability disclosure policy.

According to Melissa Vice, COO for the Department of Defense vulnerability disclosure program on the Wiley Connected Podcast, "DoD Cyber: A Conversation with Melissa Vice, COO for DoD's Vulnerability Disclosure Program," a good Vulnerability Disclosure Program should have a policy, channel, and process for responsible disclosure.

Does a security@ email alias or a web form check the box for vulnerability disclosure? What constitutes good responsible disclosure or a VDP? Can it be built in-house or are vendors a more effective route?

## Building Your Policy:

When building your vulnerability disclosure policy, you will need to align your legal, security, and IT business owners around what language should be included. Policies do not need to be long but should include these 5 elements:

1. **Promise:** The promise statement conveys your mission behind the policy's creation and explains your organization's commitment to security to customers, partners, stakeholders, the media, and others.

2. **Scope:** The scope can be as broad or as detailed as you'd like depending on how your organization is structured internally to remediate reported vulnerabilities on different assets, properties, or products.

3. **Safe Harbor:** The safe harbor statement assures that reporters of good faith will not be unduly penalized.

4. **Process:** The process guides finders on how and where to submit their reports and gives you an opportunity to ask for the information you need to quickly remediate the vulnerability.

5. **Preferences:** A living document that sets expectations for preferences and priorities regarding how reports will be evaluated. This can include the expected duration between submission and initial response, confirmation of vulnerability, additional communications during remediation, expectation of recognition, and if or when finders have the permission to publicly disclose found vulnerabilities.

Building your VDP policy page can be accomplished in house or in partnership with a vendor who has experience and a blueprint for creating policies for organizations in your business vertical. Vendors experience can expedite your policy creation process and a trusted vendor can also guide you on which areas of your business need to be involved.

## Identifying Your Channel:

Once you have an understanding of what your policy should cover, you should decide where it will live. VDPs should be easily discoverable on your website. If you choose to work with a vendor, you will also have the option of listing your VDP on their directory page which acts as a go-to listing of all VDPs available to security researchers. Being listed on a VDP directory provides more visibility from the researcher community and therefore more reported vulnerabilities.

# Process for Responding to Reported Vulnerabilities:

The most important part of a Vulnerability Disclosure Program is understanding how your team will respond to vulnerabilities. Once you receive vulnerability reports you will need to create a process to prioritize, triage, and remediate. You may also be contacted by the security researcher who submitted the report because they want to make sure it was received and as being addressed.

This is where understanding what your VDP will look like becomes paramount. Should your VDP be a security@ email alias, a web form, or should it be in the model of a hosted platform?

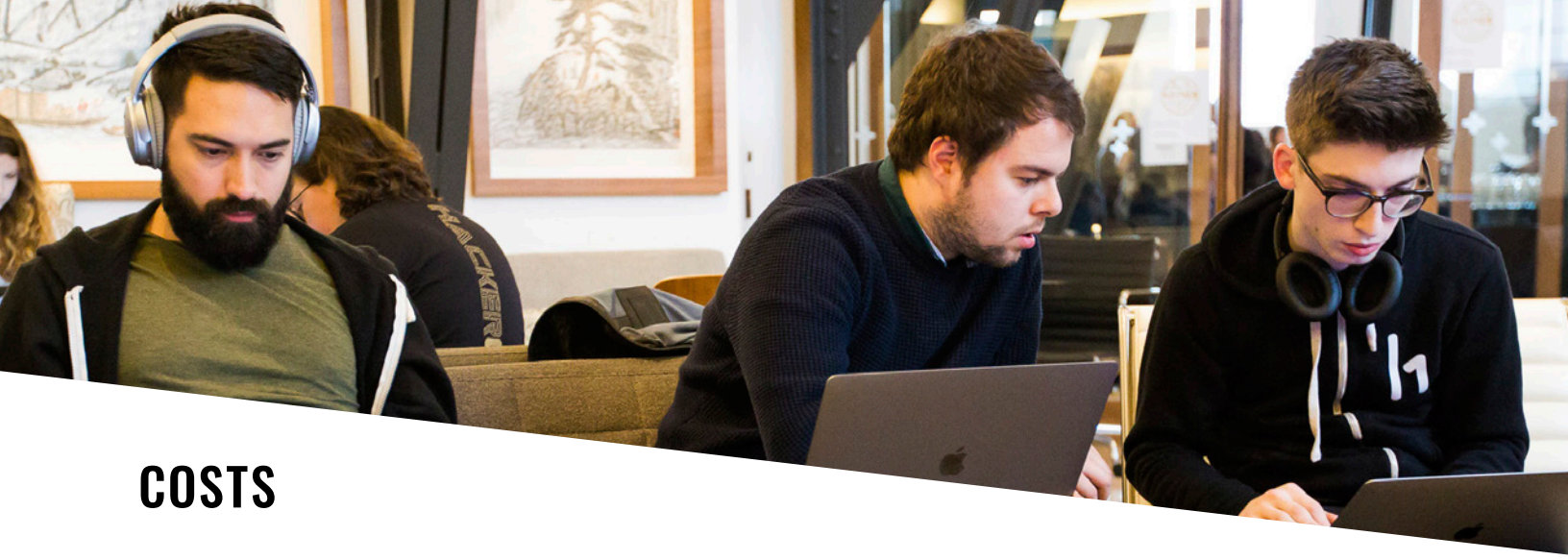
If you decide to go with listing a security@ or a personal email address on your website for vulnerability disclosure, you will then need to determine who is responsible for reading the emails, choosing which reports to address, triaging, forwarding or deleting. You will also want a method to track reports through remediation. You may receive multiple emails in regard to the same vulnerability, so you will need a process on how to consolidate and track them. You may get follow-up emails from the security researcher asking for an update. You can either set up auto responses to be sent back to the security reporter or your team can respond manually. Researchers took the time to find your email alias and report the vulnerability, so an automated response can be off putting.

A web form offers you the ability to add custom fields to get more information from security researchers that can help identify problems faster. However, like an email alias, you will still need a process for addressing the information you receive. You will still need a central repository for all of your form fills and a process to track progress and respond to researchers for follow ups or to ask more information. Most importantly, you will need a process in place for triage or understanding the validity of vulnerability which could be a cross functional effort between IT owner, business owner, and your vulnerability management team. This will need to be ironed out and tracked. Beware that some VDP vendors offer ticketing software to help organize and track reports. While ticketing systems remove some manual aspects, you will still need to triage and respond to researchers manually.

A true VDP platform acts not only as a mechanism to receive reported vulnerabilities, but can also help you store, prioritize, and track your process to remediation. It also acts as a conduit to respond directly with the security researchers who identified the vulnerability; offering them a piece of mind, and you a resource for more information - creating a positive relationship between your organization and the security researcher community. An experienced security team carefully triages each and every vulnerability report. This requires specific knowledge and understanding of both the language at hand, the package, and its context. Once the vulnerability details are verified, the team proceeds to work hand-in-hand with maintainers to get the vulnerability fixed in a timely manner.

Finally, working with a provider that is registered as a CNA (CVE Numbering Authority), it can assist with assigning the issue a CVE ID and publishing a detailed advisory. Technology lile AI/ML duplicate detection also automatically bundles vulnerabilities that have been reported by more than one researcher. Platforms offer flexibility and efficiency in the form of vulnerability workflow and tool integration, allowing your VDP to connect with other security tools like Jira, ServiceNow, GitHub, and more to fully integrate with your tech stack.

While building a VDP platform in-house can absolutely be accomplished, noting the aforementioned considerations is important.



# COSTS

Whether you choose to use an email alias, web form, or vendor for responsible disclosure, there are associated costs.

While the set up of an email alias or web form cost is low there are costs tied to managing the inbox you have set up to receive vulnerabilities. You can use a security@ email alias, but remember to decide who will get the emails, so that they do not fall between the cracks, or get forwarded to employees that shouldn't get their hands on potentially very sensitive information. Reading, organizing, tracking, and responding to the email alias can quickly become a full time job. Lack of a proper process in place for managing the inbox can also result in missed reports or being late to address the vulnerability, resulting in exploitation and serious business cost. If you receive high report volume, you may also need more resources to manage the inbox. If no additional personnel is added to maintain the VDP, the work would still need to be done and would add additional requirements on top of an already resource tapped security organization.

Like building any software, building a VDP in house requires development work, research, multiple iterations, beta testing, and QA. The salary of one software engineer alone (not including design, management, QA, etc.) is more than most VDP vendors charge for an annual license. An in-house VDP cost does not stop at development. You should also consider maintenance and management.

VDP vendors charge an annual subscription price to license their software. When selecting a VDP vendor it is important to look at what is included in the subscription cost.

- ☐ **Do they have a team that will work with you to create a policy custom to your organization, industry, and compliance needs?**
- ☐ **Do you have a communication channel and a process for communicating to third-parties?**
- ☐ **Do they have a mechanism for triaging incoming vulnerability reports, filing bugs, and communicating with researchers?**
- ☐ **Is their platform a ticketing system or custom-coded VDP?**
- ☐ **Are they trusted?**

# RISKS

There are several risks to take into consideration when building an in-house VDP or using an email alias or web submission form for vulnerability disclosure. The first being lack of experience or understanding in dealing with third party security reporters. You may need to reach out to get more details from them, or they may contact you asking for a status update. Working with an experienced vendor makes researcher communication easier because there is already a relationship with the researcher community in place. Program managers can assist you in interacting with researchers to get the right information and provide an accurate amount of feedback and incentives for reporting the vulnerability.

Another risk to going at a VDP alone is creating a process to prioritize and triage reports. Not all reports are of critical or high severity. Handling every report as an incident can lead to overreaction, wasting valuable employee time and creating a heightened state of alert for the whole organization.

Having a bad process or lack of triage processes in place can become exhausting and may result in complacency, ignoring reports, or burnout for your team. A lack of processes can also result in reports being improperly handled through a lack of communication. Reports that are unintentionally ignored may result in an unapproved public disclosure of a vulnerability and a blow to brand reputation.

Even if your team has a process in place for handling reports, this adds extra work onto already busy schedules of security and IT teams as they have to build and maintain integrations, triage/analyze reports, communicate with third parties, and remediate vulnerabilities.

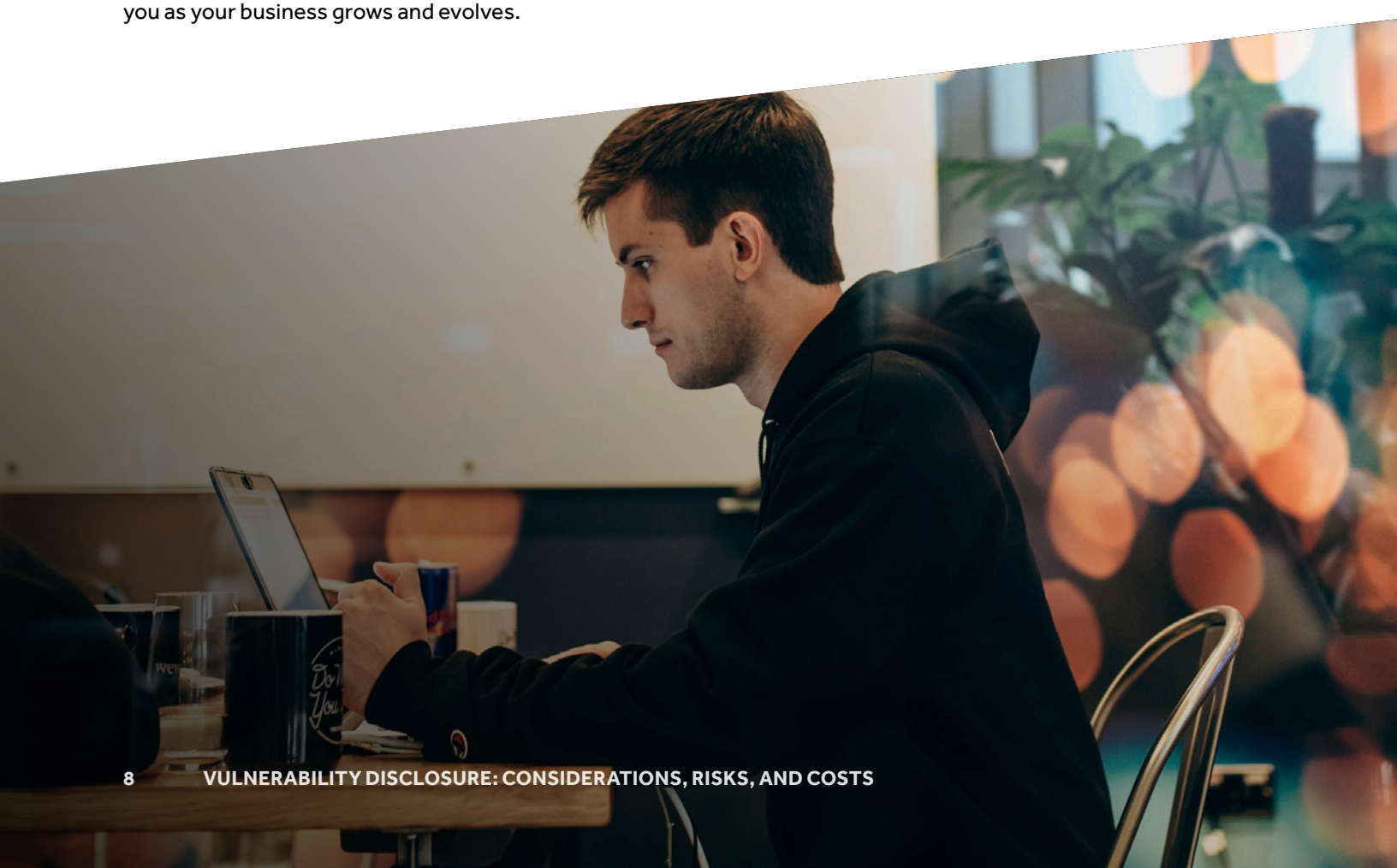
# BENEFITS OF WORKING WITH AN EXPERIENCED VENDOR

There are many benefits in going with an experienced vendor. A vendor can help you build your vulnerability disclosure policy using proven blueprints and work with your team to get all necessary stakeholders including legal, marketing, IT, and security teams on board. Vendors can also provide your VDP with extra exposure by listing it on a directory page that researchers frequent and by providing non-monetary incentives to researchers for quality reports.

Repeatability in VDP creation allows vendors to recommend best practices for process creation and workflow navigation. Their VDP platform can integrate with your security tools like ServiceNow, Jira, and GitHub. Most importantly, they can augment your security team, handling triage and analysis, so your team can focus on remediation. All of this also allows the vendor to scale with you as your business grows and evolves.

There are several considerations to keep in mind when deciding to build a vulnerability disclosure program in-house versus going with a vendor. Make sure you consider the workload in setting up and maintaining your VDP and are aware of the associated risks and costs.

Having a VDP in place greatly reduces your risk of cyber attacks by unknown vulnerabilities that could have been reported. However, not having the correct process or platform in place can still pose a risk to your organization. You don't have to go it alone. In 2020, HackerOne helped disclose over 46,000 vulnerabilities, 22% of which were high or critical. Reach out to HackerOne for more information or to get a quote on a HackerOne Response program.



# hackerone

HackerOne empowers the world to build a safer internet. As the world's most trusted hacker-powered security platform, HackerOne gives organizations access to the largest community of hackers on the planet. Armed with the most robust database of vulnerability trends and industry benchmarks, the hacker community mitigates cyber risk by searching, finding, and safely reporting real-world security weaknesses for organizations across all industries and attack surfaces. Customers include The U.S. Department of Defense, Dropbox, General Motors, GitHub, Goldman Sachs, Google, Hyatt, Intel, Lufthansa, Microsoft, MINDEF Singapore, Nintendo, PayPal, Slack, Starbucks, Twitter, and Verizon Media. HackerOne was ranked fifth on the Fast Company World's Most Innovative Companies list for 2020.