6.9 What to Do When Things Go Wrong

While we can't tell you what to do in every possible combination of contingencies that may arise in the CVD process, we can suggest the following guidelines to help you navigate the complexity.

Keep Calm and Carry On

Although problems with the disclosure process can be stressful, it's better to keep emotions in check while resolving issues. Recall from Section 2.2 that a presumption of benevolence is helpful when navigating the CVD process. As we have described thus far in Section 6, multiple things can go wrong in the disclosure process, but often these problems do not arise as a result of intentional acts of malice. So even if something has gone wrong, it's still good to give the benefit of the doubt to the good intentions of the involved stakeholders.

Avoid Legal Entanglements

Whatever the issue is in the context of a vulnerability disclosure, lawyers alone are rarely the right answer. Cease-and-desist letters tend to backfire as described in Section 6.8.

Responding with legal threats can have negative public relations effects in the long term for vendors as well:

- It gives the appearance that the vendor is more concerned about protecting its image than users' security.
- It can give the impression that the organization is bullying an individual.
- It can drive future researchers away from reporting the vulnerabilities they find.

Recognize the Helpers

For vendors: A person who shows up at your door to tell you about a vulnerability in your product is not the enemy. That person is your friend.
For researchers: A vendor who is responsive is doing better than many.

For all parties involved in CVD: Give credit where it's due. Many participants in CVD are there because they care about making things better (see Cavalry's Finder / Reporter Motivations). Recognizing them for their good work keeps them engaged and helps everybody in the long run.

Consider Publishing Early

Recall that the goal of CVD is to help users make more informed decisions about actions they can take to secure their systems. Sometimes it becomes obvious that the coordination of a disclosure has failed. In these cases, it may make more sense to publish earlier than expected than to continue to withhold information from those who could use it to defend their systems.

See also Sections 6.4, 6.5, and 6.6.

Engage a Third-Party Coordinator

We have outlined a variety of ways in which the CVD process might not go as smoothly as you'd like, whether you are a finder, reporter, vendor, coordinator, or deployer. When problems arise that you're not prepared to handle, or even if you just need a quick opinion on what to do next, there are a number of coordinating organizations available to help. These include the following:

- CERT/CC
- National CSIRTs that handle CVD cases
- JPCERT/CC
- NCSC-FI
- NCSC-NL
- Larger vendors (Google, Microsoft, etc.)
- Bug bounty operators (BugCrowd, HackerOne, etc.)

Learn from the Experience

Any process worth doing more than once is one worth improving. To that end, we recommend that participants in CVD take good notes. Hold a retrospective to identify things that went well, things that didn't, and explore changes you can make to your process for next time. This very document is in large part the result of notes taken during "lessons learned" sessions with vulnerability coordinators at the CERT/CC.

As an example of questions to begin a retrospective discussion, consider this list derived from the Scrum Alliance [1]:

- What went well?
- What went wrong?
- What could we do differently to improve?

References

1. R. Devendra, "Key Elements of the Sprint Retrospective," 24 April 2014. [Online]. Available: https://www.scrumalliance.org/community/articles/2014/april/key-elements-of-sprint-retrospective. [Accessed 23 May 2017].