

2.2. Presume Benevolence

Benevolence refers to the morally valuable character trait or virtue of being inclined to act to benefit others. In terms of the CVD process, we have found that it is usually best to assume that any individual who has taken the time and effort to reach out to a vendor or a coordinator to report an issue is likely benevolent and sincerely wishes to reduce the risk posed by the vulnerability. While each reporter may have secondary motives (such as those listed in Table 1 below), and may even be difficult to work with at times, allowing negative associations about a CVD participants' motives to accumulate can color your language and discussions with them.

This isn't to say you should maintain your belief that researcher is acting in good faith when presented with evidence to the contrary. Rather, one should keep in mind that participants are working toward a common goal: reducing the harm caused by deployed insecure systems. I Am the Cavalry describes Finder/Reporter motivations thus [1]:

Table 1: I Am the Cavalry's Finder / Reporter Motivations

Finder / Reporter Motivation	Description
Protect	make the world a safer place. These researchers are drawn to problems where they feel they can make a difference.
Puzzle	tinker out of curiosity. This type of researcher is typically a hobbyist and is driven to understand how things work.
Prestige	seek pride and notability. These researchers often want to be the best, or very well known for their work.
Profit	to earn money. These researchers trade on their skills as a primary or secondary income.
Politics	ideological and principled. These researchers, whether patriots or protestors, strongly support or oppose causes.

The Awareness and Adoption Group within the NTIA Multistakeholder Process for Cybersecurity Vulnerabilities [2] surveyed security researchers and vendors, finding that [3]:

- 92% of researchers participate in some form of CVD.
- 70% of researchers expected regular communication from the vendor about their report. Frustrated expectations were often cited as the reason for abandoning the CVD process
- 60% of researchers cited threat of legal action as a reason they might not work with a vendor to disclose
- 15% of researchers expected a bounty in return for their disclosure

< 2.1. Reduce Harm | 2.3. Avoid Surprise >

References

1. I Am The Cavalry, "5 Motivations of Security Researchers," [Online]. Available: <https://www.iamthecavalry.org/motivations/>. [Accessed 17 May 2017].
2. National Telecommunications and Information Administration, "Multistakeholder Process: Cybersecurity Vulnerabilities," 15 December 2016. [Online]. Available: <https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities>. [Accessed 17 May 2017].
3. NTIA Awareness and Adoption Working Group, "Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group," 15 December 2016. [Online]. Available: https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf. [Accessed 6 June 2017].