Vulnerability Disclosure Attitudes and Actions

A Research Report from the NTIA Awareness and Adoption Group

Contents

Executive Summary

In September 2015, the National Telecommunications and Information Administration (NTIA) convened a multi-stakeholder process to investigate software vulnerability disclosure and handling practices. The process was open to any interested participant and included members from business, government, and civil society. Members organized into three working groups to study different aspects of vulnerability disclosure and handling. This report is a product of the "Awareness and Adoption Working Group," which focused on increasing understanding and use of best practices.

To assess the state of the field, the working group surveyed populations of software vendors and security researchers. Questions focused on past or current behavior for reporting or responding to vulnerabilities, as well as processes that worked or could be improved. There were 414 responses to the researcher survey and 285 to the vendor survey. Key findings from each are summarized below.

Researcher survey

- The vast majority of researchers (92%) generally engage in some form of coordinated vulnerability disclosure.
- When they have gone a different route (e.g., public disclosure) it has generally been because of frustrated expectations, mostly around communication.
- The threat of legal action was cited by 60% of researchers as a reason they might not work with a vendor to disclose.
- Only 15% of researchers expected a bounty in return for disclosure, but 70% expected regular communication about the bug.

Vendor survey

- Vendor responses were generally separable into "more mature" and "less mature" categories. Most of the more mature vendors (between 60% and 80%) used all the processes described in the survey.
- Most mature technology providers and operators (76%) look internally to develop vulnerability handling procedures, with smaller proportions looking at their peers or at international standards for guidance.
- Mature vendors reported that a sense of corporate responsibility or the desires of their customers were the reasons they had a disclosure policy.
- Only one in three surveyed companies considered and/or required suppliers to have their own vulnerability handling procedures.

This data can help guide future efforts to increase awareness and adoption. In particular, efforts to improve communication between researchers and vendors should encourage more coordinated, rather than straight-to-public, disclosure. Removing legal barriers, whether through changes in law or clear vulnerability handling policies that indemnify researchers, can also help. Both mature and less mature companies should be urged to look at external standards, such as ISOs, to better understand cost-savings across the software development lifecycle from the implementation of vulnerability handling processes.

Introduction

What is a vulnerability?

Vulnerabilities are weaknesses of software, hardware, or online services that can be used to damage the confidentiality, integrity, or availability of those systems or the data they store. Finding these vulnerabilities and informing affected parties is essential to protect our economy and citizens.

As software and technology systems become increasingly interconnected and complex, the likelihood they will contain vulnerabilities increases. As these systems become integrated into a vast array of products and services, the potential for those vulnerabilities to negatively impact users in profound ways is becoming more significant. Vulnerabilities create opportunities for malicious attackers to commit cybercrime or disrupt user activity. Although vendors seek to identify and remediate vulnerabilities before their products and services are brought to market, testing for everything is impossible. As a result, vulnerabilities may still be found in technology products and online services, either through intentional investigation or accidental discovery. When vulnerabilities are identified, a clear path for security researchers or discoverers to "disclose" their findings to technology developers, manufacturers, and service providers helps to resolve issues without exposing users to undue risk. A clear path is often part of an organization's "vulnerability handling" policy, process, or program.

Much work has previously been undertaken to develop best practices for vulnerability disclosure and handling. Many of these best practices have even been captured in two International Standards Organization (ISO) standards, ISO/IEC 29147[1] and ISO/IEC 30111[2]. These best practices and ISO standards are built on the notion that a coordinated approach to vulnerability disclosure is beneficial to all stakeholders – technology manufacturers, operators, users, and security researchers. However, not all technology providers or security researchers have fully embraced the principles underlying coordinated vulnerability disclosure. Discussions about vulnerability disclosure processes have a history of veering toward the dogmatic, which can undermine trust between the security research and technology provider communities. We often hear negative, outdated assumptions voiced by each side about the other.

Assumptions, particularly erroneous ones, undermine our ability to understand the heart of the problem, which reduces our chances of proposing solutions that will work. Assumptions and stereotypes are also clear signs of a lack of trust, making it considerably harder to create a collaborative environment and drive adoption of better practices. This hurts both technology providers (in terms of reputation) and security researchers (due to fear of legal threats), and also hurts technology users, as vulnerabilities in technology put them at risk.

The assumptions and prejudices that impede collaboration between researchers and technology providers may be based on past experience, but that doesn't mean they are correct in every setting or scenario. Even if they were previously correct, they may not be any longer. The technology landscape is constantly evolving, and technology providers, users, and researchers learn more every day. For example, the emergence of the Internet of Things (IoT) is a huge shift, introducing masses of complex, interconnected technologies and requiring new industry sectors to address concerns around secure product design. Similarly, policy and regulatory developments, such as the Digital Millennium Copyright Act (DMCA) exemption for security research[3] and the Food and Drug Administration (FDA) post-market guidance for medical devices[4], also have significant impact.

To get beyond the hyperbole and assumptions, we launched two surveys to investigate current, real world attitudes about vulnerability disclosure and handling. Our goal was to investigate: 1) how broad the adoption of established practices is; and 2) where barriers to adoption may exist. We hoped to ground our understanding of today's ecosystem so that we could make meaningful recommendations to drive increased adoption. We surveyed the two main stakeholder groups involved: security researchers, who may report potential vulnerabilities to technology providers and operators; and technology providers and operators, who may receive reports about potential vulnerabilities.

The surveys and this report were developed and disseminated by the "Awareness and Adoption Group" participating in a multi-stakeholder process on vulnerability disclosure and handling, convened by the National Telecommunications and Information Administration (NTIA).[5] The Awareness and Adoption Group includes representatives from technology providers, the security research community, civil liberties groups, and others involved or interested in the vulnerability disclosure and handling lifecycle. The Awareness and Adoption Group benefited from the contributions of a number of individuals and organizations, including: BSA | The Software Alliance, The Center for Democracy and Technology, CERT Coordination Center, Dino Dai Zovi (security researcher), Nick Leiserson (Office of Representative James Langevin), Katie Moussouris (co-editor of ISO 29147 & ISO 30111 and CEO of Luta Security), Microsoft, Neal Krawetz (security researcher), New America's Cybersecurity Initiative, Rapid7, and SAP[6].

[1] http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170

[2] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231

[3] https://www.ftc.gov/news-events/blogs/techftc/2016/10/dmca-security-research-exemption-consumer-devices

[4] http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[5] https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

[6] The views expressed in this report are the result of a collective effort of the Awareness and Adoption Group, but may not represent the views of the individual contributors.

Response and Demographics

As the Awareness and Adoption Group is a volunteer effort, cost efficiency, speed, and practicality were priorities for our method of gathering data. As such, we created online surveys, which we promoted through a variety of means, including press, social media, personal networks, outreach to industry associations, etc. We realized our outreach methods meant that we would likely encounter a selection bias – those taking the surveys would likely already have some familiarity with, or interest in, the topic. We made efforts to promote the surveys within more diverse communities, including through outreach to vertical industry information sharing and policy groups representing sectors that tend to have relatively less experience with vulnerability disclosure and handling. However, we want to be transparent: we expect the data presented below to have a bias toward those that have dealt with vulnerability disclosure in some way in the past. More information on the survey methodology and related challenges is included as Appendix A.

Despite these challenges, we saw a generally positive response to both surveys and are pleased to report that we had 414 respondents to the researcher survey, and 285 to the technology provider and operator survey. Analysis of the data reveals we had almost no fake or intentionally misleading responses. In addition, analysis of the data revealed a number of meaningful findings, which are discussed in the following sections.

With regard to demographics for the 414 responses to the security researcher survey, just over half of respondents (210) were from the United States. The remaining 204 security researchers hailed from 50 other countries; their self-identified locations are depicted in chart 1.

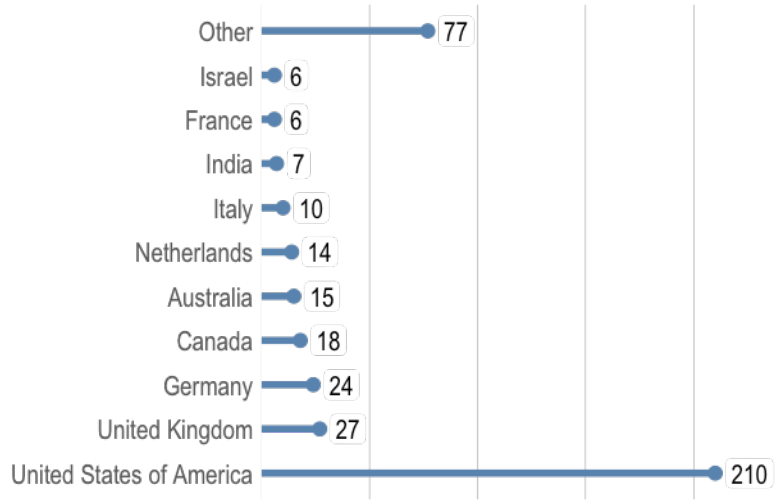

Chart 1: Geographical breakdown of respondents to Researcher survey

We also asked security researchers to describe how they typically research or find vulnerabilities, i.e. as part of their regular employment or in another capacity; respondents could identify more than one context. The largest portions of respondents reported researching independently (50.6%) or on behalf of a for-profit organization (42%). In addition, 17.2% of respondents described themselves as "accidental finders," and 8.6% reported researching on behalf of a not-for-profit organization.

With regard to demographics for the 285 respondents to the technology provider and operator survey, a significant majority of respondents (180) were from the United States. The remaining 105 respondents self-identified as being from 29 other countries, including, in order of significance: Canada, Germany, Japan, the United Kingdom, France, and Australia.

As chart 2 depicts, most respondents were from the technology sector, though arguably any company responding to the survey could have self-identified as a technology company.

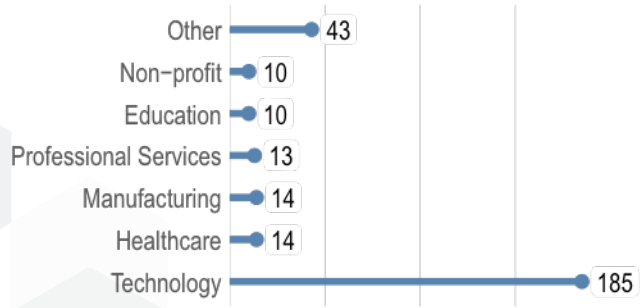

Chart 2: Industry breakdown of respondents to Technology Provider and Operator survey

We received responses from companies that represent a good mix of sizes in terms of employee number. Specifically, 160 respondents were from "small" companies (with fewer than 1,000 employees), and 125 respondents were from "large" companies (with 1,000 or more employees). However, a significant majority of respondents were from "very small" (with fewer than 100 employees) or "very large" (with 10,000 or more employees) organizations.

Key Findings and Analyses – Researcher Survey

Coordination beats going solo

The researchers surveyed overwhelmingly utilized coordinated disclosure as their typical method of revealing vulnerabilities. The majority of security researchers typically engaged with vendors directly, while one-quarter worked with a third party, either a coordinating organization or a third party Product Security Incident Response Team (PSIRT). Only 4% of researchers typically made vulnerability disclosures in public fora, such as conferences. Sadly, an additional 4% did not typically reveal vulnerabilities that they discovered.

This data demonstrates a strong awareness of the value of sharing vulnerability information with technology providers and operators.

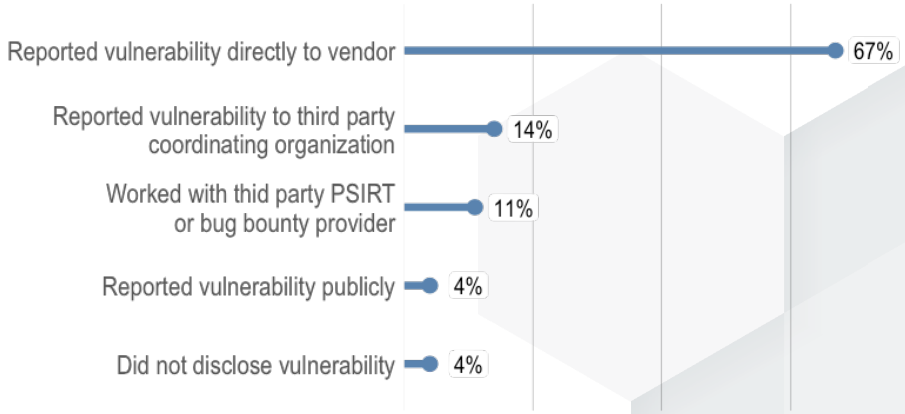

Chart 3: Reporting paths for security researchers

Communication is key

Although awareness of the first step in coordinated vulnerability disclosure practices (i.e., reporting to a technology provider or operator directly or a coordinating third party) was high among survey respondents, other coordinated vulnerability disclosure practices were not always followed by security researchers. More than one-quarter of researchers surveyed have shared a vulnerability publicly because a timeline for response was not met. An additional 20% considered sharing a vulnerability publicly because timelines lapsed. Chart 4 depicts responses to a question about security researchers' expectations for the process of reporting vulnerabilities to vendors directly as well as they typical behavior and experiences in interacting with vendors (see Appendix B, Question 5B for full question).

In other words, despite planning initially to disclose a vulnerability in a coordinated manner, nearly half of all researchers at some point considered disclosing publicly due to frustrated expectations. Chief among those expectations is that technology providers and operators will provide notification to the security researcher when the issue is resolved; 95% of respondents anticipated at least that level of communication. But fully two-thirds also expected regular updates on the investigation of, and progress in, mitigating their reported vulnerability.

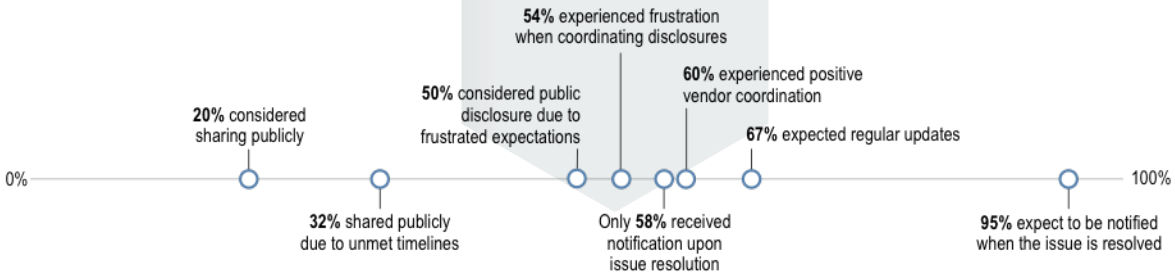

Chart 4: Expectations and behaviors of security researchers

What is coordinated vulnerability disclosure?

Coordinated vulnerability disclosure is a set of practices based on a view that collaboration between researchers and technology providers/operators is essential to protecting users. In a coordinated disclosure model, security researchers report vulnerabilities either directly to the relevant technology provider/operator or to a coordinating third party, such as an appropriate government entity. The technology provider/operator then coordinates and communicates with the reporter of the vulnerability throughout the investigation and remediation of the vulnerability. Finally, the researcher and technology provider/operator coordinate in disclosing the vulnerability publicly.

As long as the technology provider/operator is responsive to the reporter and there is no evidence of an attack using the vulnerability in the wild, coordination in disclosure means that the reporter of the vulnerability does not disclose it until a fix or other mitigation has been developed. If the reporter discloses the vulnerability ahead of a fix, then the reporter and technology provider/operator at least coordinate in describing a full range of possible mitigations, putting users in the most empowered position to operate their technology securely.

84% of researchers were available to answer vendor questions about their reports.

Communication with vendors was a mixed bag. While 60% of respondents indicated that they had experienced productive coordination with vendors, 54% had also experienced frustration when attempting to coordinate on a disclosure. And despite the vast majority of researchers expecting notification on issue resolution, only 58% received it.

Timelines were also very important to the researcher community, with over nine in ten respondents describing a desire for some deadline for remediation. However, the timeframe involved is not always perceived as something that should be fixed. On the contrary, only 18% of the researchers that expressed an expectation of a resolution timeline thought that vendors should conform to a timeline without regard to the circumstances of a particular bug. Maintaining a definite resolution date, then, is less important than communicating the decision-making involved in determining resolution priority in a transparent manner, allowing a researcher to calibrate their expectations.

Finally, the surveyed population seemed to understand the need for bidirectional communication: 84% of researchers were available to answer vendor questions about their reports.

From an adoption standpoint, one barrier seems to be a lack of resiliency in best practices should communication between researcher and vendor break down. Many researchers felt strongly that disclosing vulnerabilities publicly was the remedy to frustrated expectations. Having strong fallback mechanisms as part of a framework may help ensure that the principles of coordinated vulnerability disclosure are more broadly adopted.

Legal concerns remain a barrier

While most of the surveyed population typically reports vulnerabilities, security researchers expressed concerns about several factors that caused them to hesitate before reporting. Chief among these – a concern of three out of five researchers – is that they may be subject to legal proceedings if they disclose their work. While it is undoubtedly important that researchers have a firm understanding of the law governing their activities, coordinated disclosure is harmed if researchers believe that revealing the flaws they've discovered could expose them to legal risk. Though, according to the broader data, fear of legal action is not a barrier per se, it may cause researchers to deviate from their default choices on disclosure. Increasing legal certainty, therefore, is a method that may improve adoption of best practices.

Chart 5: Fear of legal threats against security researchers

60% of respondents feared they may be subject to legal proceedings if they disclose their work.

Rewards matter – but not to everyone

A slim majority of respondents (53%) expected at least an acknowledgement of their contribution in return for notifying a vendor of a vulnerability. However, one in five expected nothing at all in return for disclosure, and 14% actively preferred to remain anonymous. Beyond acknowledgement, only 15% of researchers expected to be paid for their efforts in the form of a bounty or other economic reward. While the survey did not delve into whether monetary incentives drove bug hunters to examine particular products, it is clear from the results that bounties have not become an expected norm in the surveyed researcher community.

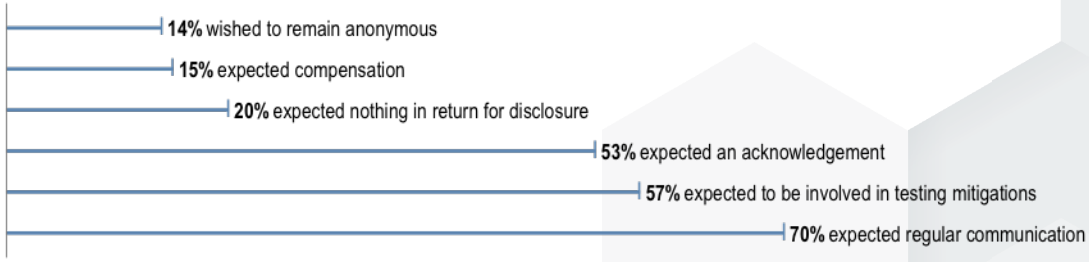

Chart 6: Expectations of security researchers

On the other hand, researchers do expect to be communicated with throughout the investigation and remediation of the bug. In particular, 70% of researchers indicated that this level of communication was to be expected "in return for disclosing a vulnerability," which indicates that communication is viewed not just as a way to more efficiently eliminate bugs, but also as recompense for the time that researchers put into vulnerability discovery. Beyond the regular updates discussed in the communications section, many researchers (57%) also expressed an expectation that they would be able to test any mitigations released in response to the vulnerabilities they identified.

> Communication is viewed not just as a way to more efficiently eliminate bugs, but also as recompense for the time that researchers put into vulnerability discovery

Key Findings and Analyses – Technology Provider and Operator Survey

The findings from the technology provider and operator survey indicated a spectrum of "vulnerability maturity" for respondents, and analysis of the results enabled us to distinguish between "more mature" and "less mature" organizations. We performed a multiple correspondence analysis (MCA) on seven of the survey responses: best practices, vulnerability handling processes, disclosure process (2 questions), whether vulnerability reports inform security development processes, and what prevention steps are employed. MCA enables analyzing the pattern of relationships across all these variables, and we wanted to see if the data had natural "maturity" groupings so we could tag each respondent with this label and look at the results through such a lens.

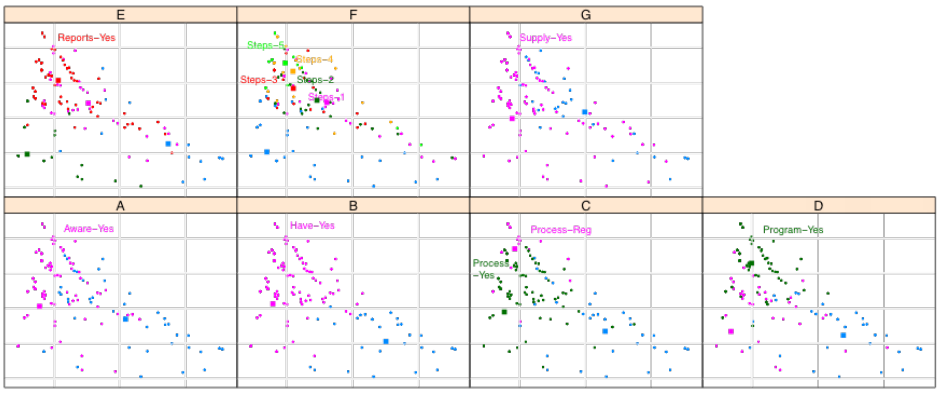

Chart 7: Multiple correspondence analysis clusters

The MCA clustering algorithm mapped all seven variables down to x/y coordinates — one for each respondent — and chart 7 highlights the areas where more disciplined or mature practices are employed for each answer. We then identified a combined region that encompassed the intersection of each grouping and used that to tag a respondent as "more mature" or "less mature."

Sources of disclosure policies

Most respondents confirmed that they are aware of vulnerability handling practices, and very few indicated that they are unsure of what to do next. Given that awareness of the survey is a prerequisite for taking it, this is perhaps not surprising.[7] However, there are still insights to be gleaned from understanding how companies that do plan for vulnerability handling approach the challenge.

The most common answer regarding awareness and sources of vulnerability handling best practices (see Appendix C, question 4) was that organizations had looked internally to examine their own processes. This held across all organization sizes and maturity levels, although more mature companies were by far the most likely (76%) to have completed such internal reviews. In contrast, just over half of mature companies examined their industry peers, and only two in five had reviewed the ISO vulnerability disclosure and handling standards. Even more significant, though, is the finding that fewer than 20% of less mature companies took any of these three steps.

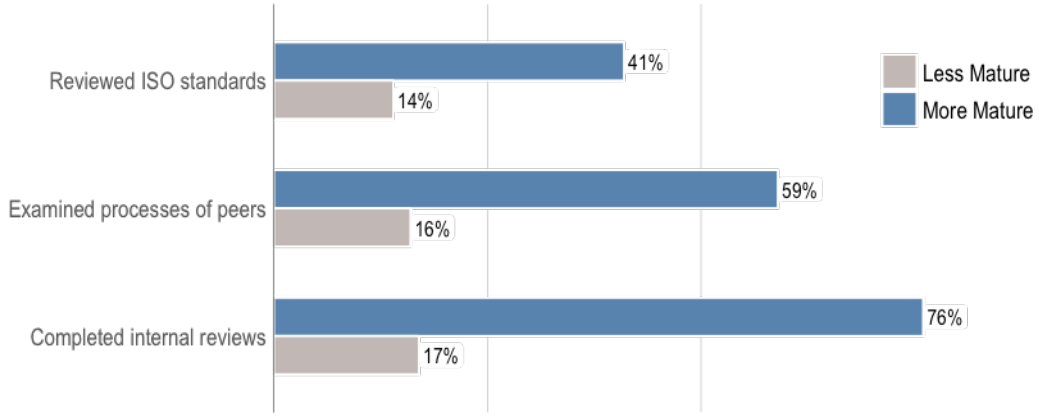

Chart 8: Sources of best practices for technology providers and operators

More mature companies may identify as having an understanding of what to do about vulnerability handling, but based on the survey data, that understanding derives from their own experiences rather than a set of standard policies. In addition to raising the level of maturity among vendors then, broader adoption of best practices may hinge on companies looking outward rather than internally only.

Creating the right process

When asked what, if any, vulnerability disclosure and handling processes technology providers and operators have in place, no strong favorites emerged. On the contrary, with the exception of bug bounty programs, the majority (between 60% and 80%) of mature companies used all of the processes described in the survey. In fact, the most commonly selected policy/process was the most comprehensive, describing the existence of a dedicated path for receiving, triaging, and mitigating vulnerabilities.

> The most commonly cited process was comprehensive, encompassing a dedicated path for receiving, triaging, and mitigating vulnerabilities

[7] It is hard to quantify how broad adoption of basic vulnerability disclosure and handling processes is across all technology providers and operators; however, we believe that the vast majority of organizations do not have clear and established processes in place. HackerOne provides some insight into this, though their data is now over a year old and policy changes such as the DMCA exemption for security research and the FDA post-market guidance may have affected it. "A whopping 94 percent of Forbes' Global 2000 have no established channel for receiving external vulnerability reports. Of the top 100 publicly traded companies in the Global 2000, only 13 percent have disclosure programs." https://hackerone.com/blog/vulnerability-disclosure-assistance

What is striking in the findings is the vast gulf between more mature and less mature companies. Much of this is by design: the answers to this question (Appendix C, question 5) were used to sort the respondents by maturity. The majority of more mature companies used at least two of the best practices described. Less mature companies used zero or one. But the responses clearly indicate that maturity of a vulnerability handling policy is not very continuous, at least with respect to the questions asked in the survey. In encouraging adoption, then, one of the goals may be to drive companies past a maturity threshold at which point they are likely to incorporate a number of best practices into their policies.

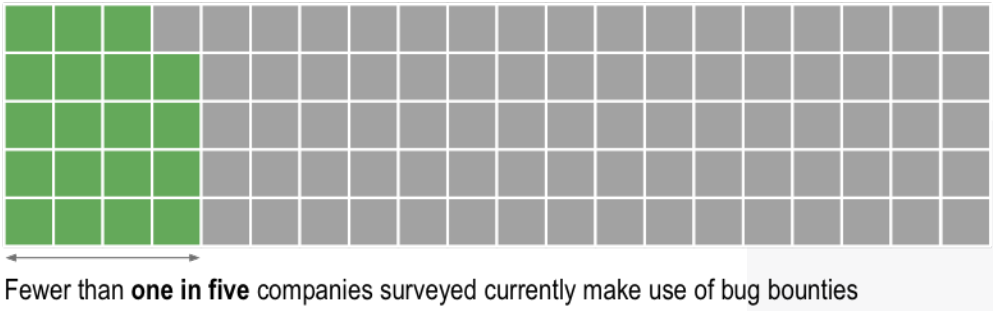

Chart 9: Adoption of bug bounties

As noted, the existence of a bug bounty program was the sole example of a process or program not used by the majority of mature respondents. Bug bounty programs have been relatively widely covered in the media; however, as fewer than one in five mature companies surveyed currently make use of them, it may be worthwhile to clarify in messaging that sound vulnerability disclosure practices are not contingent upon offering remuneration for bugs.

What is a bug bounty?

A bug bounty program is an initiative that sets out to incentivize security researchers to disclose vulnerability discoveries to the manufacturer or operator of the affected technology. The goal is to enable the technology provider or operator to address or mitigate the bug before the general public is aware of them and there is widespread abuse or exploitation of the issue. In order to do this, bug bounty programs offer financial rewards to researchers for vulnerability disclosure, often contingent upon the severity of the bug. They also create a safe environment for disclosure, making it clear what the legal boundaries and expectations are for research.

Bug bounties may offer a fixed or fluid amount of money, be time-bound or ongoing, and have other terms of eligibility. They have slowly started to become more prominent over the last few years. Bugcrowd has documented a trickle of bug bounty programs since 1995 and the establishment of an upward trend in 2013. https://bugcrowd.com/resources/history-of-bug-bounties

Responsibility dominates economics

Mature companies utilize vulnerability disclosure frameworks for three primary reasons. Four out of five respondents (to Appendix C, question 6) indicated that they developed the policies because their customers care about security. It is unclear whether companies feel that a vulnerability handling policy is viewed by their customers as a proxy for solid security practices, or whether the existence of such policies materially improves security in a way that is evident to customers; however, it is clear that demand from customers, real or perceived, can alter companies' behavior.

Chart 10: Customer demand drives adoption of best practices

Similarly, two-thirds of mature respondents reported that they have implemented vulnerability handling procedures because they view it as "part of [their] corporate social responsibility." The survey is limited in its ability to determine the causality relationship here: namely, whether companies first introduced the vulnerability handling process because of a drive toward corporate social responsibility, or whether it has subsequently become the justification or benefit of the program. Nonetheless, it may help drive adoption of practices to understand that responsibility – both to the customer and as a corporate citizen – is the primary reason reported for having vulnerability handling processes in place.

Responsibility – both to the customer and as a corporate citizen – is the primary reason reported for having vulnerability handling processes in place

Direct economic benefits were cited by just over half of the respondents as another motivation for utilizing vulnerability handling policies. Specifically, 54% of more mature companies reported that vulnerability disclosure and handling policies actually reduced the costs of marketing and development of their software products and services. To further encourage adoption, it may be worthwhile to expand awareness of this advantage to using best practices.

54% of more mature companies reported that vulnerability disclosure and handling policies actually reduced the costs of marketing and development of their software products and services

Nascent third party risk mitigation

When asked how they prevent or mitigate the risk of vulnerabilities in products or services provided through their supply chain, only one-third of respondents, both large and small, considered and/or required suppliers to have vulnerability handling processes or procedures in place. One in four companies indicated they had plans to work with suppliers to ensure resolution of vulnerabilities in their products, with another fifth indicating that they passed third-party vulnerabilities onto vendors, or to a coordinating body.

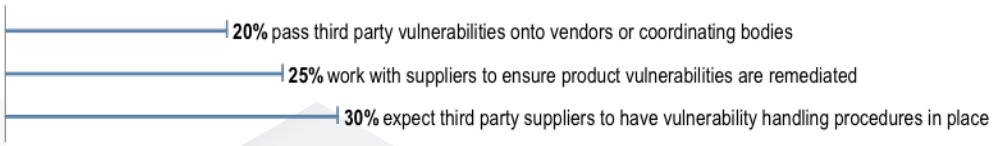

Chart 11: Handling third-party vulnerabilities

These findings are interesting juxtaposed with the responses about the reasons for adopting vulnerability handling best practices: notably, survey participants view disclosure policies as something their customers want more often than they look to similar practices among their suppliers. Addressing this gap may be an effective way to drive adoption of coordinated disclosure policies. It may also engender more focus on incorporating multi-party disclosure into handling procedures, because companies that considered suppliers' stance toward vulnerability handling were also more likely to coordinate with those suppliers on vulnerability (see Appendix C, question 10).

Coordinating Disclosure for Improved Outcomes

We conducted the surveys to challenge our assumptions, and we did indeed find some surprises. For example, there is a great deal of discussion in the security community around the efficacy and impact of bug bounties. The survey results suggest that perhaps the key benefit of bug bounty programs for researchers is less about receiving financial rewards, and more about the formalization of disclosure and communication processes. This helps create a safer environment in which to conduct research and disclose findings, with clear parameters outlined for what is permissible.

A theme that emerged clearly throughout the results of both surveys is that, for many of our respondents, the benefits of a coordinated approach to vulnerability disclosure and handling are understood and appreciated. Both researchers and more mature technology providers are willing to invest time and resources into collaborating so they can create more positive outcomes for technology consumers.

While we recognize that this response may be partly skewed due to the selection bias in developing the surveyed population, we hope it may be indicative of a larger trend, or at least highlight the potential for collaborative approaches to be adopted more broadly. However, this outcome is contingent on increased awareness of the issue and the benefits of a coordinated approach to vulnerability disclosure and handling, particularly among less mature technology providers. The survey results provide some guideposts for communicating with providers, and, thankfully, recent events and initiatives are already increasing awareness and making the concept of vulnerability disclosure and handling less niche. The DMCA exemption passing, publication of guidance by government regulators, and the launch of high-profile vulnerability handling and bug bounty programs by leaders such as the Department of Defense[8] and General Motors[9] are all important steps in the right direction.

That said, more work is needed to continue increasing awareness of the necessity and value of vulnerability disclosure and handling. And more efforts must be made to understand and remove the barriers to adoption of best practices. The Awareness and Adoption Group hopes to continue on this mission and we welcome participation from anyone interested in helping. Everyone reading this report has the potential to drive awareness of this issue forward, and if you have ideas on how to encourage greater adoption of best practices, please contact NTIA-AA [at] googlegroups [dot] com. We look forward to continuing to promote a dialogue among those interested in protecting users and the technology ecosystem.

---

[8] https://hackerone.com/deptofdefense/

[9] https://hackerone.com/gm

Appendix A – Challenges of Methodology

As indicated above, we recognize that a certain amount of selection bias for respondents was built into the means and process of the surveys. As a result, we oriented our questions more toward adoption of established and recommended practices, rather than toward questions related to awareness. You can find both surveys reproduced in full in Appendices B and C below.

Additional challenges

During the development of the surveys, we considered issuing a third survey to gather insight into the views of technology consumers. We ultimately decided against this for two main reasons:

- The 'technology consumer' category is vast, and we would literally have been surveying the entire internet. As a result, we felt it was very unlikely that we would generate meaningful findings out of the survey responses.
- Given limited resources of time and budget, there was even less likelihood of avoiding selection bias with a consumer survey than there was with the other two categories. Any responder that we reached with a consumer-centric survey would almost certainly have an interest in security well beyond that of an average consumer.

We anticipated receiving responses to the technology provider survey from the community of open source technology projects and providers, but instead, we received extensive feedback from this community that the survey questions were too oriented towards commercial providers. Were we to disseminate similar surveys again, we would draft a separate survey for the open source community, or at the very least get more open source community input on crafting the questions for the technology provider survey. We owe a huge thank you to those in the open source community who spent the time and expended the effort to give us detailed feedback and apologies to the broader open source community for not adequately addressing their particular operating context with the surveys.

In addition, we discovered some weaknesses in the survey question format as we assessed responses. For instance, some questions intentionally allowed for multiple responses because we wanted to capture the range of experiences that communities may have in interacting with each other over time. However, in some instances, that flexibility also made the data difficult to interpret. A telling example is the responses that we received from security researchers on a question about their experiences interacting with technology providers and operators. A majority (54.7%) said that their communication with technology providers/operators was mostly frustrating, and a majority (60.7%) also said that their communication with technology providers/operators was mostly productive.

We also discovered that the data identifying the industry sector for technology providers was somewhat skewed as we had not taken out "technology" as an option in the auto-generated list of industries.

We have provided these details above in the interests of transparency and hopefully as a helpful guide to anyone considering a similar endeavor in the future. While the challenges shaped the data we were able to collect, we do not believe they negate the value of that data, nor the learnings therein.

Appendix B – Researcher Survey

1: Where is you located? (Auto-generated geolocation options)

2: What best describes the way in which you do most of your security research? (pick the one that is most frequently the case when you disclose vulnerabilities)

[ ] I research on behalf of a not-for-profit organization (i.e. a university).

[ ] I research for a security product or assessment service that I sell or that my organization sells.

[ ] I research as a part of my organization's regular software development or IT lifecycle.

[ ] I research on my own time and for my own self-motivated reasons.

[ ] I'm not a security researcher, but I occasionally stumble across vulnerabilities.

3: Have you previously disclosed a vulnerability? (yes/no)

4: Have you used or referenced any of the following while writing a vulnerability notification? (pick all that apply)

[ ] CVE

[ ] CVSS

[ ] CWE

[ ] CPE

[ ] OWASP

[ ] Static or dynamic analysis tools

[ ] Fuzzers

[ ] Tools that scan for known vulnerabilities (i.e. exploit testing frameworks)

5: How have you disclosed/do you typically disclose vulnerabilities? (pick one that best represents your usual behavior)

- I did not disclose or report the vulnerability.
- I reported the vulnerability publicly, without first reporting to the vendor or a third party (i.e. on a blog, to a user group, on a public forum or mailing list, or at a conference).
- I reported the vulnerability to a third party coordinating organization (e.g. CERT/CC, JPCERT/CC).
- I worked with a third party PSIRT, bug bounty provider, or other organization (such as HackerOne, Bugcrowd, or ZDI) to report my vulnerability.
- I reported the vulnerability to the vendor directly.

5B: If you report vulnerabilities to vendors directly, please tell us about your expectations for the process, your behavior, and what has transpired or typically transpires (pick the responses that best represent your usual expectations, behavior, and experiences with vendors):

- I did not seek or expect information in return.
- I expected regular updates regarding the vendor's investigation and progress.
- I expected notification when the issue was resolved.
- I expected the vendor to tell me how the vulnerability was fixed and to let me test the fix.
- I received updates and progress reports from the vendor.
- I received notification from the vendor when the issue was resolved.
- The vendor contacted me with questions about my report.
- I was available to answer questions from the vendor about my report.
- I gave the vendor a timeframe for a response, and that timeframe was met.
- I gave the vendor a timeframe for a response, and that timeframe was not met, so I seriously considered sharing the vulnerability publicly but ultimately did not.
- I gave the vendor a timeframe for a response, and that timeframe was not met, so I shared information about the vulnerability publicly.
- The vendor provided a timeframe for response, and that timeframe was met.
- The vendor provided a timeframe for response, and that timeframe was not met, so I seriously considered sharing the vulnerability publicly but ultimately did not.
- The vendor provided a timeframe for response, and that timeframe was not met, so I shared information about the vulnerability publicly.
- My communication with the vendor was mostly productive, and we coordinated well.
- My communication with the vendor was mostly frustrating, and we did not coordinate well.

Please provide a brief explanation of your answer/s to #5B if you are comfortable doing so (again, all information will be

anonymized). [[comment box]]

6: What are your expectations on the time it takes to fix a vulnerability? (pick one)

[ ] I expect the vulnerability to be fixed by a timeline set by me or by the vendor.

[ ] I have no rigid timelines, but I expect the vendor to prioritize high-risk vulnerabilities, communicate with me throughout an extended investigation and remediation process, and fix the vulnerability within a reasonable timeline considering the circumstances.

[ ] I do not care.

7: What are your expectations in return for disclosing a vulnerability? (pick the response/s that best represent your usual expectation/s)

[ ] I do not expect anything.

[ ] I expect that the vendor will communicate with me during the investigation of—and, if relevant, the resolution of—the vulnerability.

[ ] I expect a statement giving me credit.

[ ] I expect a monetary reward.

[ ] I do not want anyone to mention me. I prefer to be anonymous.

8: What, if any, reasons for hesitation occur to you when considering whether to disclose or report a vulnerability that you have discovered? (check all that apply)

[ ] I am concerned that I may be threatened with legal action.

[ ] I am concerned that my employer will not support me.

[ ] I am concerned that the research community will not support me.

[ ] I am concerned about the possibility of stumbling upon confidential information that I should not have accessed (e.g. pirated software, private or personally identifiable information, and information that results in potential copyright infringement or license violation).

[ ] I am worried that my disclosure may be used by miscreants (i.e., exploits may be developed and used for nefarious purposes).

[ ] I fear for my own security (i.e., that I may become a target for attacks).

[ ] I worry that I may have to invest too much time or too many resources throughout the vulnerability investigation and fix testing processes.

Please provide a brief explanation of your answer to #7 if you are comfortable doing so (again, all information will be anonymized). [[comment box]]

Appendix C – Technology Provider and Operator Survey

Section 1: Tell us about your organization

(reminder, all information is anonymized and aggregated)

1: What industry do you operate in? (Auto-generated vertical options)

2: What size is your business? (Auto-generated size options)

3: Where is your business located? (Auto-generated geolocation options)

Section 2: Vulnerability disclosure

4: Is your organization aware of vulnerability handling best practices, such as ISO standards or other widely discussed and agreed practices? (pick all that apply)

- No, we are not aware of this issue
- Yes, vaguely – but we don't know what to do next
- Yes – but that's not a priority for us, and we haven't taken any concrete actions to move beyond our general level of awareness
- Yes – we have looked at how other companies are handling vulnerabilities
- Yes – we have examined the ISO standards on the topic
- Yes – we have worked internally to examine our organization's vulnerability handling practices

5: Does your organization have a vulnerability handling policy or process? (pick all that apply)

- We do not have anything in place for this
- We have an alias for reporting vulnerabilities
- We have a published policy for handling vulnerabilities
- We have a dedicated and monitored path for reporting as well as resources for investigating, triaging, and coming to a resolution on reported vulnerabilities
- We acknowledge reporters of vulnerabilities if they want that recognition
- We have a bug bounty program
- We alert or notify our consumers about vulnerability fixes
- We inform and/or coordinate with other vendors that may be affected by vulnerabilities that have been reported to us.
- We indicate where we fix vulnerabilities (supported products) as well as where we do not (unsupported or discontinued products)

6: If your organization does have a vulnerability disclosure process in place, please tell us why: (pick all that apply)

- N/A
- Our customers care about security, and so do we
- Regulations demand that we have such a process
- We're concerned about liability
- We consider this part of our corporate social responsibility
- Having a mature process in place ultimately reduces other costs of developing and marketing secure products and services
- We see this as a way of getting free quality assurance testing for our products
- Vulnerability disclosures can help drive innovation in our technology

Comment box: Please provide brief details if you are comfortable doing so (again, all information will be anonymized):

7: If your organization does not have a vulnerability disclosure process in place, please tell us why: (pick all that apply)

- N/A
- We're not very familiar with or don't know much about this issue
- We want to do something but are not sure what the right approach would be for our organization

- We want to do something but don't have the resources we need to do so
- It costs our business too much
- Our development lifecycles are not suited to this
- Our customers don't care, so it's not a priority for us

Comment box: Please provide brief details if you are comfortable doing so (again, all information will be anonymized):

Section 3: Secure product development

8: Do vulnerability reports inform your security development lifecycle, helping to prevent futures vulnerabilities in your products and services? (pick one answer that best represents what your organization typically does or tries to do)

- N/A
- Yes, we feed learnings from reports back into our software development process, helping to prevent similar vulnerabilities or issues in future products and services
- No, we deal with reports as one-off instances

Comment box: Please provide brief details if you are comfortable doing so (again, all information will be anonymized):

9: What steps do you take to prevent vulnerabilities in your products and services? (pick all that apply)

- We develop software and/or hardware with security in mind, using a security development lifecycle process.
- We track and work towards company-wide conformity with security development lifecycle policies and processes.
- We comply with or leverage recognized international cybersecurity best practices, such as ISO/IEC 27001 and the NIST Cybersecurity Framework.
- We use pen testing and devote resources to fixing issues discovered through such testing.
- We train employees on the importance of utilizing cybersecurity best practices in product and service development.

10: How does your organization prevent or mitigate the risks of vulnerabilities in products or services provided through your supply chain? (pick all that apply. If your organization has not experienced this, pick any that represent how you would approach it.)

- We do not take into consideration the approach that our suppliers take with regard to vulnerability handling.
- We consider whether our suppliers have vulnerability handling policies/processes.
- We require, by contract, that our suppliers have vulnerability handling policies/processes.
- We do not acknowledge or forward reports of vulnerabilities that affect a supplier's products or services.
- We tell security researchers to contact the relevant suppliers rather than our organization about vulnerabilities affecting a supplier's products or services.
- We forward any supplier product/service-related vulnerability reports that we receive on to our relevant suppliers.
- We forward any supplier product/service-related vulnerability reports that we receive on to a coordinating organization, such as CERT/CC.
- We work with our suppliers to ensure that vulnerability reports are received, investigated, and triaged and that suppliers come to an appropriate resolution on reported vulnerabilities.

Comment box: Please provide brief details if you are comfortable doing so (again, all information will be anonymized):