451 Research | BLACK & WHITE PAPER

Exploring Coordinated Disclosure

SHEDDING LIGHT ON PERCEPTIONS AND EXPERIENCES IN HOW SOFTWARE VULNERABILITIES ARE REPORTED

COMMISSIONED BY

VERACODE

You change the world, we'll secure it.

SEPTEMBER 2019

About this paper

A Black & White paper is a study based on primary research survey data that assesses the market dynamics of a key enterprise technology segment through the lens of the "on the ground" experience and opinions of real practitioners — what they are doing, and why they are doing it.

ABOUT THE AUTHOR

DAN KENNEDY

RESEARCH DIRECTOR, VOICE OF THE ENTERPRISE: INFORMATION SECURITY

Daniel Kennedy is the Research Director for Information Security for 451 Research's Voice of the Enterprise (VoTE) quantitative research product, where he is responsible for managing all phases of the research process. He is an experienced information security professional who has written for both Forbes online and Ziff Davis, has provided commentary to numerous news outlets including The New York Times and The Wall Street Journal, and his personal blog Praetorian Prefect was recognized as one of the top five technical blogs in information security by the RSA 2010 Conference.

Table of Contents

Executive Summary

Few topics in information security engender as impassioned a response from security practitioners as vulnerability disclosure. The website Attrition.org maintained a *16-year list* of ill-advised corporate reactions to the identification of vulnerabilities in their products or services that ranged from threats made to a security researcher's employer, questionable Digital Millennium Copyright Act takedown requests, and direct legal threats. The issues faced by researchers led the Electronic Frontier Foundation to publish a *Coders' Rights Project* to advise security researchers on legal threats to their work. Yet perspectives have shifted over the past decade and a half, as identified by this survey of security and technology professionals that included developers, IT security, third-party penetration testers and independent security researchers with a variety of responsibilities.

Veracode commissioned this survey from 451 Research to understand how widely accepted and practiced coordinated disclosure – whereby a security researcher identifies a flaw and notifies the company, then the two work together to fix and publicly disclose the flaw – really is and where the pain points reside. In addition, we wanted to explore the means organizations have established to receive vulnerability reports, and the attitudes toward a coordinated disclosure policy on both sides of the organization and among external security researchers. We also sought a deeper understanding of the motivations of security researchers, actions when a vulnerability is identified, timing for disclosure, desired outcomes, how organizations structure disclosure policies, and the effectiveness of bug bounties.

Key Findings

- Most (90%) respondents see vulnerability disclosure as a public good, that the identification of vulnerabilities increases transparency and is good for the overall security posture for everyone.
- More than one-third (37%) of organizations have received an unsolicited disclosure report in the past 12 months.
- For those organizations that received an unsolicited vulnerability report, 90% of vulnerabilities were disclosed in a coordinated fashion between security researchers and organizations.
- A majority, 62%, do not think prior permission from a product or application owner is required.
- In general, respondents don't believe that a contracted security researcher should be disclosing vulnerabilities (70% percent).
- Three out of four organizations report having an established method for receiving vulnerability reports from security researchers.
- While most organizations maintain a process to receive vulnerability reports as an aspect of due care, at least a third are motivated by the fear of full disclosure of the vulnerability.
- Only 9% of respondents who have identified a security vulnerability went the full-disclosure route. Communication (e.g., notification when a fix is applied, cited by 57% of respondents) and collaboration (e.g., the ability to validate a fix, 37%) are the expectations of security researchers when they take the time to report a vulnerability.
- Nearly half (47%) of organizations have implemented bug bounty programs, but they say that only 19% of vulnerability reports come via bug bounty programs.
- Only 63% of open source vulnerabilities reported are being fixed.

Methodology

To gather relevant data for this report, 451 Research conducted survey from December 2018 to January 2019 using a representative sample of 1,000 respondents across a range of industries and organization sizes in the US, Germany, France, Italy and the UK. Survey respondents reported enterprise roles such as application development, infrastructure and information security, as well as security consultants, third-party vulnerability assessors or penetration testers, and independent security researchers. Respondents were required to have an average to high level of familiarity with vulnerability disclosure models to participate.

Brief History of Vulnerability Disclosure

The debate on vulnerability disclosure has persisted for decades in the modern era – and much longer than that if one takes into account similar calls for accountability. The locksmith Alfred Charles Hobbs was making the case for publishing weaknesses in lock design in 1853. In 1965, Ralph Nader published *Unsafe at Any Speed,* in which he detailed perceived inadequacies in automobile safety, and faced a harassment campaign from the automotive industry as a result. The Bugtraq mailing list started in 1993 as a method of full disclosure, publishing information on a flaw without restriction, for security vulnerabilities.

The debate remains an impassioned one because of the varying interests involved: security researchers' desire to see the vulnerability fixed relatively quickly and to receive updates from a vendor vs. an organization's desire to make a fix before it's disclosed and to not appear to be putting users at risk. In limited or no-collaboration scenarios, organizations are not willing to work with security researchers, or vice versa, or communication breakdowns prevent a mutually agreeable disclosure process. We must also consider the users of the technology that can simultaneously benefit from and be put at risk by the disclosure of vulnerabilities.

The term 'responsible disclosure' entered the lexicon in 2001 when a security manager for Microsoft compared full disclosure to anarchy. It's important to note Microsoft's central position in this debate; in the early 2000s, the Windows operating system and related software held an even more dominant position in the market than it does today, and Patch Tuesday became an operational responsibility in many enterprise security programs.

> "IT'S HIGH TIME THE SECURITY COMMUNITY STOPPED PROVIDING BLUEPRINTS FOR BUILDING THESE WEAPONS. AND IT'S HIGH TIME COMPUTER USERS INSISTED THAT THE SECURITY COMMUNITY LIVE UP TO ITS OBLIGATION TO PROTECT THEM. WE CAN AND SHOULD DISCUSS SECURITY VULNERABILITIES, BUT WE SHOULD BE SMART, PRUDENT, AND RESPONSIBLE IN THE WAY WE DO IT."
>
> **SCOTT CULP, 2001**[1]

1 https://web.archive.org/web/20011109045330if_/http://www.microsoft.com:80/technet/treeview/default.asp?url=/technet/columns/security/noarch.asp

As early as 2002, Steve Christey and Chris Wysopal (@WeldPond) were proposing processes that recognized the required interplay between vulnerability reporter and the organization maintaining the code in their responsible vulnerability disclosure process proposal to the IETF. This included aspects of what constitutes a more 'coordinated' disclosure, including the need to coordinate agreement on a release date for a patch or fix, as well as the need to provide credit to the reporter.

In 2007, Bruce Schneier made the argument that responsible disclosure was only possible under the threat of full disclosure, and that public scrutiny is the only lever that's effective at getting software companies to close security holes:

> "BEFORE FULL DISCLOSURE WAS THE NORM, RESEARCHERS WOULD DISCOVER VULNERABILITIES IN SOFTWARE AND SEND DETAILS TO THE SOFTWARE COMPANIES – WHO WOULD IGNORE THEM, TRUSTING IN THE SECURITY OF SECRECY. SOME WOULD GO SO FAR AS TO THREATEN THE RESEARCHERS WITH LEGAL ACTION IF THEY DISCLOSED THE VULNERABILITIES…IT WASN'T UNTIL RESEARCHERS PUBLISHED COMPLETE DETAILS OF THE VULNERABILITIES THAT THE SOFTWARE COMPANIES STARTED FIXING THEM."
>
> **BRUCE SCHNEIER**[2]

In 2010, a Google researcher, Tavis Ormandy, provided detailed information on an unpatched Windows vulnerability after being dissatisfied with Microsoft's inability to commit to a 60-day window for correction. This was controversial for a few reasons, not least of which being that Ormandy worked for a competitive company, but one of the accusations that was leveled was that he had violated the concept of 'responsible disclosure.' He responded:

> "THE IMPORTANT IMPLICATION OF REFERRING TO THIS PROCESS AS 'RESPONSIBLE' IS THAT RESEARCHERS WHO DO NOT COMPLY ARE SEEN AS BEHAVING IMPROPERLY. HOWEVER, THE INVERSE SITUATION IS OFTEN TRUE: IT CAN BE IRRESPONSIBLE TO PERMIT A FLAW TO REMAIN LIVE FOR SUCH AN EXTENDED PERIOD OF TIME."
>
> **TAVIS ORMANDY**[3]

Later in 2010, Microsoft sought to retire the term 'responsible disclosure' in favor of 'coordinated vulnerability disclosure,' because the former implied a value judgement about behaviors in security research. In the words of then senior security strategist Katie Moussouris:

> "WE DON'T WANT AN EMOTIONALLY LADEN TERM CLOUDING THE DEBATE, AND THAT'S DEFINITELY GOTTEN IN THE WAY OF A LOT OF GOOD DISCUSSIONS BETWEEN LIKE-MINDED PEOPLE IN SECURITY."
>
> **KATIE MOUSSOURIS, 2010**[4]

2 *https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html*
3 *http://googleonlinesecurity.blogspot.com/2010/07/rebooting-responsible-disclosure-focus.html*
4 *https://www.theregister.co.uk/2010/07/22/microsoft_coordinated_disclosure/*

Despite an evolving discussion a quarter century in the making, the reception Nader received from the automotive industry is a familiar experience for researchers in the security industry. The website Attrition maintained a long list of examples of legal or related threats from 2000 to 2016 detailing organizations' attempts to quash the dissemination of security vulnerability research they felt damaging or embarrassing. This approach has historically resulted in a Streisand effect where the research gets more attention than it originally would have, yet communication breakdowns and mistakes in dealing with security researchers remain common. For example, in just the time this survey was conducted:

- *The Wall Street Journal* reported a teenager and his mother's frustrations in trying to inform Apple of a vulnerability with FaceTime.[5]
- A Tenable Research researcher gave up on trying to contact PremiSys after multiple attempts in 90 days, and disclosed vulnerabilities with its physical access card system.[6]
- A researcher alleges he was assaulted by the COO of a vendor that makes kiosks used in casinos following a strange saga where the FBI brokered a meeting between two security researchers and the vendor.[7]

5 *https://www.wsj.com/articles/teenager-and-his-mom-tried-to-warn-apple-of-facetime-bug-11548783393*
6 *https://www.tenable.com/blog/multiple-zero-days-in-premisys-identicard-access-control-system*
7 *https://www.csoonline.com/article/3338112/vendor-allegedly-assaults-security-researcher-who-disclosed-massive-vulnerability.html*

Today's Perceptions of Disclosure

The disclosure debate has matured over 25+ years in a modern information security context but is hardly settled. When asked for their vulnerability disclosure preference, more than half of survey respondents said they favor security researchers working with the code maintainer or vendor responsible for the vulnerable technology. Of those, 39% want a fix in place for the vulnerability before disclosure happens, regardless of how long it takes to make that fix. The other 17% said full disclosure should happen if a vendor is not responding to the researcher in a timely manner. Forty-five percent of respondents still favor immediate full disclosure, and perhaps surprisingly given their position as the maintainers of code, application developers favor full disclosure at a percentage greater than the rest of the sample, at 48%.

Figure 1: Vulnerability disclosure preferences

Source: 451 Research 2019 Collaborative Disclosure survey
Q: : What is your preference for vulnerability disclosure for products you manage?

Vulnerability Disclosure as a Public Good

Nearly half (48%) of the respondents to this study believe vulnerability disclosure represents a public good, that companies should both be transparent about their security posture and held publicly accountable for flaws. A bit fewer, 42%, were more conservative in their stance, noting that improvements in security have a side benefit, and organizations should make efforts toward such improvements, but those organizations should not be subject to either public pressure or regulatory scrutiny because of vulnerability disclosure.

Keep in mind this survey examines the perceptions of technical people working within companies that write code and support applications for both internal operations and customers – in other words, people whose work lives are affected by having to respond to a publicly disclosed security flaw. Would nearly half of the same have identified third-party vulnerability disclosure as a public good in 2001 or 2010?

With 90% of respondents confirming that disclosing vulnerabilities publicly serves a broader purpose of improving how software is developed, used and fixed, it is analogous to a similar turning point in the automobile industry. For decades after the invention of the automobile, manufacturers became better at improving speed, durability and functionality, but safety was

neglected at first. Automobile manufacturers were even reluctant to include safety features in their vehicles for fear of delays in delivery to consumers. Yet common sense prevailed – the industry was forced to alter vehicles to include safety features such as anti-lock brakes, airbags, seatbelts and collision impact studies as part of the process of building the vehicles. Today, anyone would agree that these safety improvements are in the best interest of the public. The software industry is encountering an inflection point – the impact on global business interests, consumer opinion and geopolitical stability is significant when software is vulnerable to attack. But software companies and security researchers are near universal in their beliefs today – collaborating to disclose vulnerabilities to improve software security is good for everyone.

Solicited Versus Unsolicited Testing

A majority of survey respondents said they believe a third-party security researcher should be able to do unsolicited testing (62%), but differences in respondent populations emerged at both the industry and role level. When comparing industry verticals, 74% of respondents working for finance organizations said they support the idea of unsolicited testing, whereas more than half of those (53%) in government organizations said such testing should *not* take place. As with full disclosure, those responsible for making changes to applications are more bullish: 71% of application developers responded 'yes' to security researchers doing unsolicited testing. This may seem counterintuitive; developers would likely be most impacted in having their workflow interrupted to make an emergency fix. Despite that – and it may be due to the way modern application development is conducted or community experience with the workflow of open source projects – developers seem to expect to have their work tested outside the organization and ready to respond to problems that are identified.

Regional differences also emerged; the most notable was that 82% of respondents from Germany indicated that security testing without permission was permissible, which was considerably higher than the study average. While there are differences in general attitudes toward privacy and technology between, for example, the EU and the US, this targeted difference may be due to the GOd data leak that exposed the personal data and communications of several German politicians in January, while this survey was being fielded. If so, that adds a layer to the results; the recency of a well-publicized cyberattack may swing perceptions in favor of unsolicited, third-party security testing.

The study tested the resolve of the 70% of survey takers who said that a security researcher hired to test an application should not disclose a vulnerability publicly by presenting a series of scenarios where an attack on a system would be highly impactful to its users. For example, 64% of those who originally said 'no' switched to thinking that disclosure is a good idea if the vulnerability found is in a medical device that maintains life or health, a pacemaker for example. Well over half (60%) changed their answer to 'yes' if the vulnerability affected the safe operation of transportation, such as an automobile, an intergenerational nod to *Unsafe at any Speed*. More than half, 56%, said disclose regardless of the situation when critical infrastructure such as the electrical grid is involved.

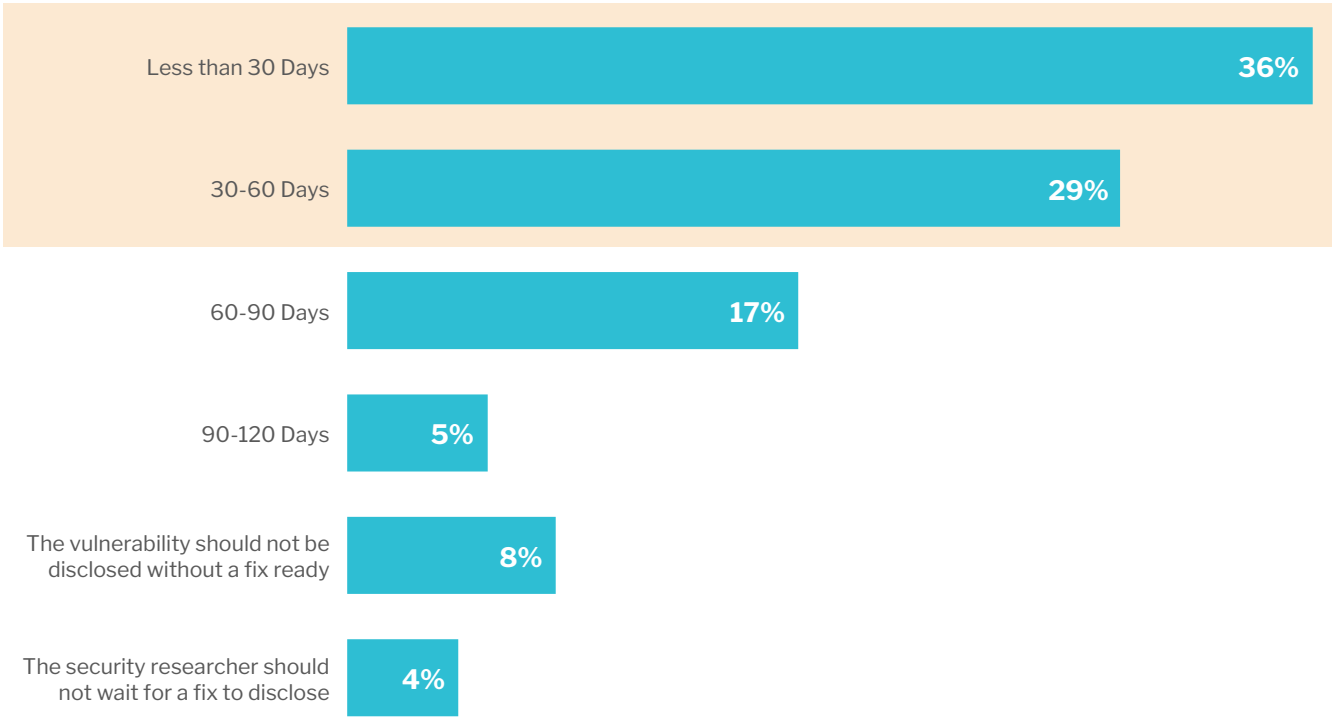
Disclosure Timelines

In one of the disclosure examples cited earlier, Google's Ormandy cited 60 days as the deadline for vulnerability correction. Google Project Zero later amended that to a 90-day deadline, and that duration is often informally cited as a standard by those in the industry. However, 65% of survey respondents, including a significant percentage of enterprise personnel who would be responsible to such timelines in providing a fix, said that less than 60 days is the appropriate time frame. In total, more than one in three respondents (36%) said they believe that organizations should correct a vulnerability in less than 30 days.

Figure 2: Appropriate time frame for a vendor to correct a vulnerability once notified

Source: 451 Research 2019 Collaborative Disclosure survey

Q: What's an appropriate time frame for a vendor to correct a vulnerability once notified, before the security researcher discloses it?



Disclosure Experiences

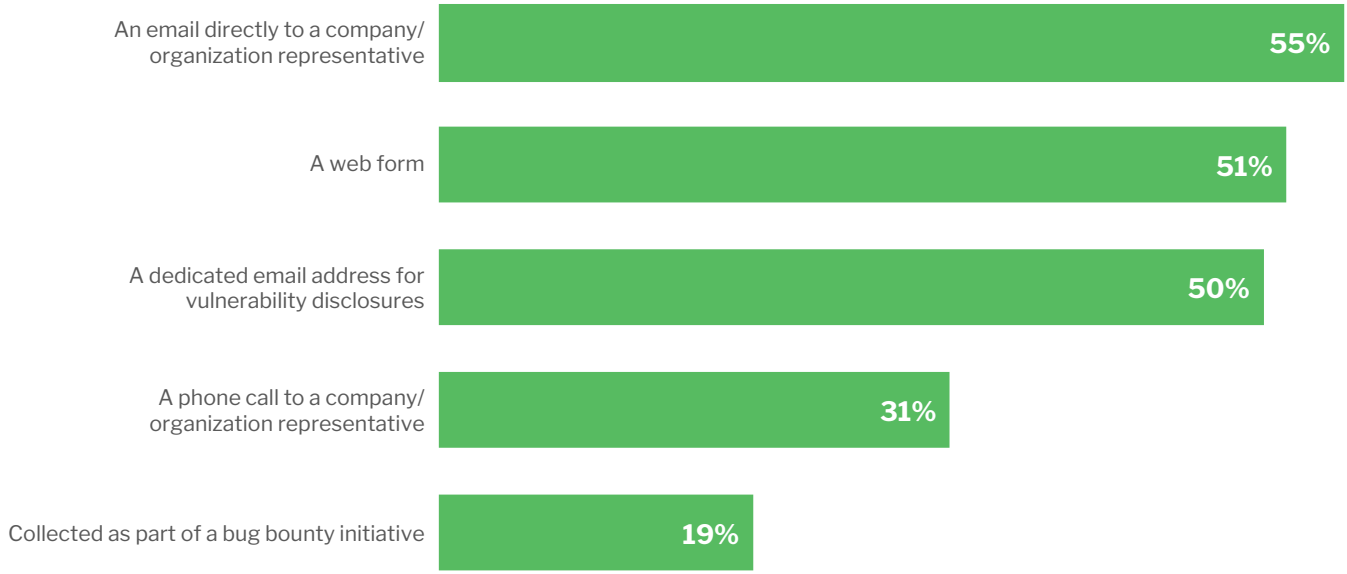
Organizational Experience

Given the general level of acceptance of the idea of third-party security testing and vulnerability disclosure as, if not universally agreed upon as a public good, at least acknowledged as an operating reality, it is perhaps unsurprising that 75% of surveyed organizations claimed to have a process in place for receiving a vulnerability report. And it's encouraging to see that vulnerability reports are happening with great frequency – 37% of organizations reported receiving a vulnerability report, unsolicited, in the last 12 months.

Of those respondents who have received a vulnerability report in the last year, 90% coordinated the process of vulnerability disclosure with the security researcher that found the vulnerability, and 10% did not. In general, the process was found to be a positive one when rated on a 1-5 scale, where 1 is extremely positive and 5 is extremely negative, with the survey average coming in at a score of 2. That said, 12% of survey respondents were neutral, and 10% viewed the coordinated vulnerability disclosure experience as negative.

Figure 3: Method used to make vulnerability submission

Source: 451 Research 2019 Collaborative Disclosure survey
Q: What method was used to make the vulnerability submission?



The most common trigger for this coordinated vulnerability process, in a little over half of the cases, was an email to the organization. Similarly, half received vulnerability reports via researchers filling out a web form or using an email address specifically set up to receive such reports. One-third of the cases kicked off with a phone call. In only 19% of cases was the vulnerability received as part of a bug bounty process. This finding is illuminating because it disputes the notion that bug bounties are a viable or even preferred way for organizations and security researchers to collaborate on vulnerabilities. It also sheds new light on the motivations of researchers who report vulnerabilities – the majority are not financially motivated (see Bug Bounties section below).

Figure 4: Motivation for developing a process for receiving vulnerability disclosures

Source: 451 Research 2019 Collaborative Disclosure survey

Q: Which of the following best describes your organization's motivation for developing a vulnerability-disclosure-receiving process?

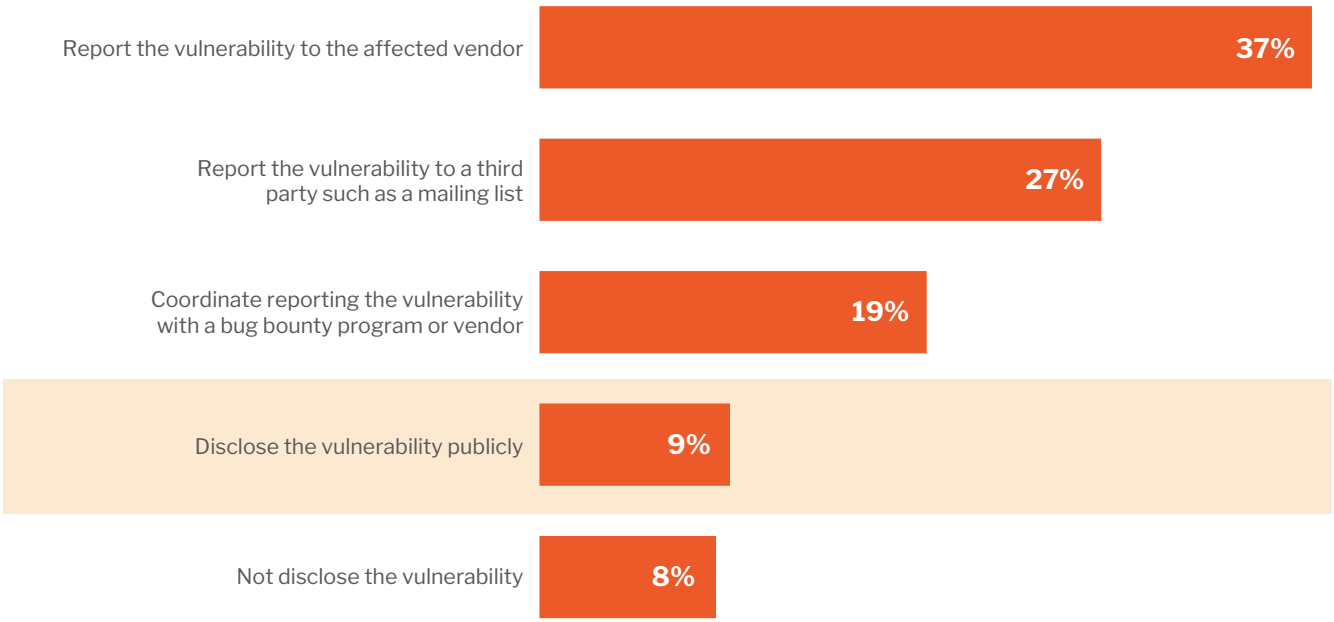
For those organizations that have instituted a process for receiving reports of security vulnerabilities, the primary motivations fall somewhere on a continuum between a desire to do the right thing and fear, the latter of which strengthens the argument cited earlier that coordinated disclosure historically has been facilitated under the threat of full disclosure.

Vulnerability Reporter Experience

Forty-one percent of respondents to this study reported having personally identified a security vulnerability in a third-party product. Only 9% of them took the full-disclosure route, disclosing the vulnerability publicly instead of reporting the vulnerability to the vendor (37%). A mediating party (27%), or a bug bounty program or vendor (19%) was much more common. Security flaws in open source followed a similar trajectory: 48% of respondents with open source software in place have identified a vulnerability in their open source software and reported it to the open source project, and 17% fixed the security defect themselves. The most common response from the open source project upon receiving the vulnerability report was to fix the problem (63% of the time); 20% of the time a ticket was opened, and 11% of the time more information was requested. In only 6% of cases was the report ignored.

Figure 5: Action when security vulnerability is identified

Source: 451 Research 2019 Collaborative Disclosure survey
Q: In the most recent vulnerability you identified, did you…?

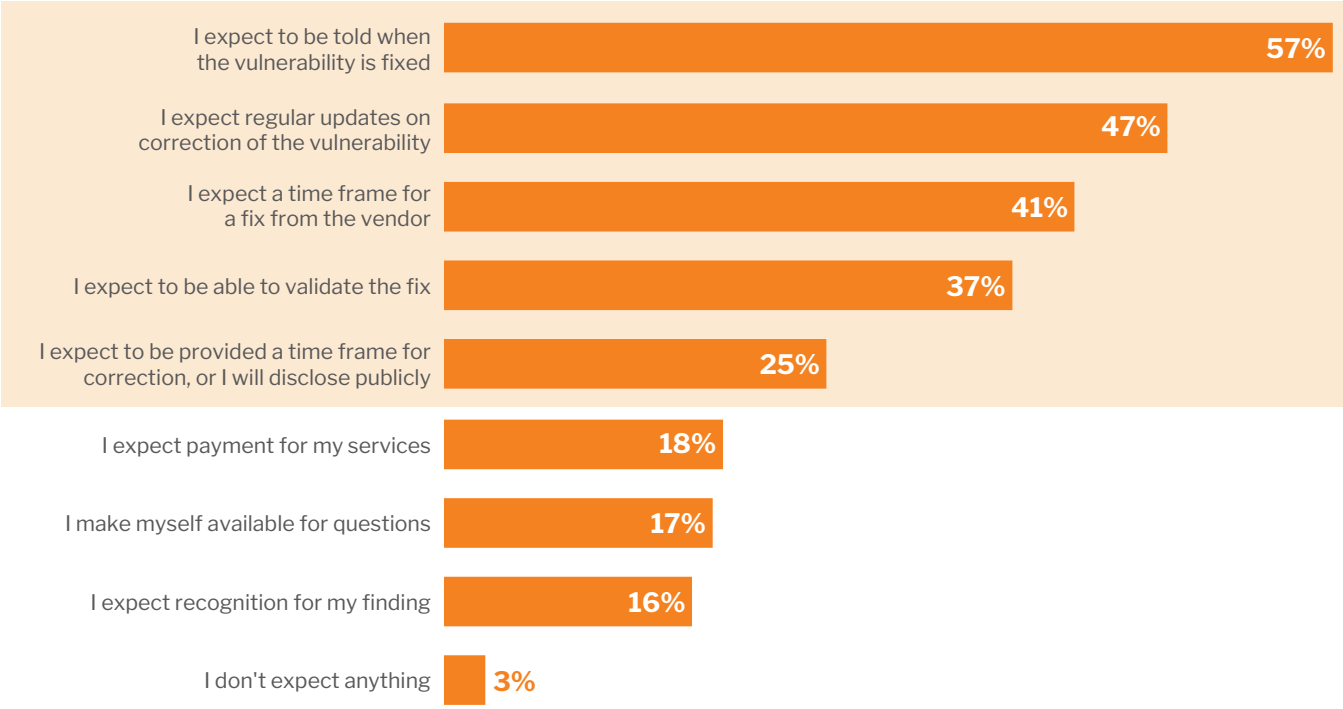


Although most failures in a coordinated vulnerability disclosure process occur because a software vendor won't respond to a vulnerability report, other failures occur beyond acknowledgement when the needs of security researchers are not met. The results can be that the defect is disclosed, or more subtly, for example, that researchers are less likely to participate in the process the next time they find a vulnerability. Thus, meeting the expectations of third-party researchers is important, and for the most part, these expectations are not all that complicated to meet.

The most common answers to what a security researcher expects after submitting a vulnerability report come down to ongoing communication. Most expect to be told when a vulnerability is corrected. Others expect a timeline for the fix and regular updates. Thirty-seven percent expect to be able to validate that the fix works, which ostensibly also benefits the software vendor. A quarter explicitly noted that they will pursue full disclosure if not provided a timeline for correction of the vulnerability. Only 18% of third-party security researchers said they are looking for some sort of payment, and only 16% expect explicit recognition.

Figure 6: Expectations when a vulnerability is reported

Source: 451 Research 2019 Collaborative Disclosure survey
Q: When you report a vulnerability to a vendor, what are your expectations?



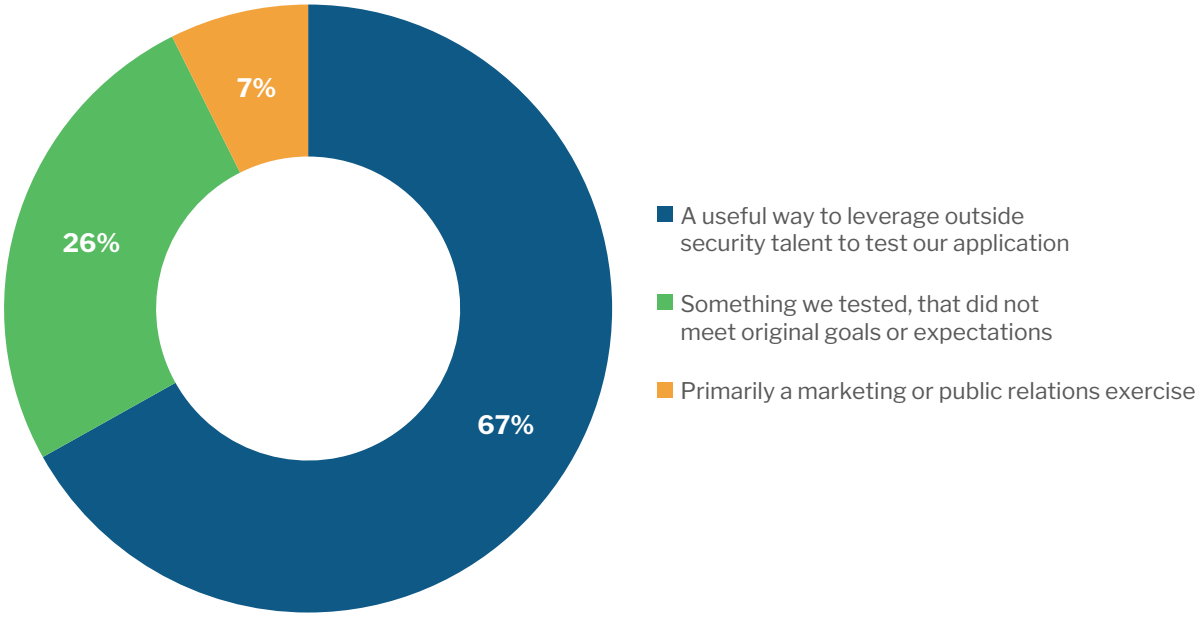
Bug Bounties

Bug bounties represent a way to incentivize third-party security researchers to work with vendors by offering compensation for finding security vulnerabilities in their software. This compensation can come directly from a company or via a broker, and it can represent a way to extend security testing capabilities as well as direct unsolicited third-party testing toward an outcome more beneficial to the tested organization.

There have been documented problems with this approach. One is disagreement over the value of vulnerabilities found. Yahoo!, for example, at one point sent T-shirts to researchers who successfully found vulnerabilities. In 2016, Uber attempted to quiet news of a breach of 57 million users' personal data by paying a $100,000 ransom under the guise of it being a bug bounty. Still, with high-profile organizations such as Google and the Department of Defense running bug bounty programs, this approach to leveraging third-party security research has grabbed more than its fair share of attention in recent years. The lure of a big payday may drive headlines, but according to our survey, researchers are much more invested in having the vulnerability corrected than any compensation or recognition.

Figure 7: Thoughts about experience with bug bounties

Source: 451 Research 2019 Collaborative Disclosure survey
Q: What do you find the bug bounty program to be?



Nearly half (47%) of survey respondents' organizations have worked with bug bounties at some level. Of those that have, 67% felt that it was a useful way to leverage security talent that lived outside of their organizations, 26% felt that the experience did not meet their expectations, and 7% felt that doing a bug bounty was primarily a marketing or public relations exercise, so lacked tangible security value and was done more from an advertising or virtue-signaling perspective.

One of the most important aspects of running a successful bug bounty program is being prepared to receive, act on and respond to vulnerability reports. At a high level, this takes the form of validating findings in a timely manner and correcting identified problems. On a 5-point scale where 1 represents 'totally unprepared' and 5 represents 'completely prepared,' the average response among those organizations that had some experience with bug bounties was a 4, an indication of being somewhat prepared to receive reports and make fixes.

While bug bounties have been mostly successful undertakings, they aren't the solution to finding and disclosing every flaw. Coordinated disclosure should be accepted across the industry as a standard whereby vulnerabilities can be shared and discussed without fear of reprisal by either side, not centered on a bug bounty program, which is not sustainable long-term. Coordinated disclosure will lead not only to more secure software but greater information sharing, which builds a more cohesive community of developers and security teams and security researchers working together toward a common goal of finding and fixing flaws.

Conclusion and Recommendations

The comfort level with the idea of third-party security testing, even unsolicited testing, among those who develop, support and secure applications suggests that such activities should be approached as a constant at this point, essentially both a cost of doing business when leveraging technology and an aspect of due care. Resisting third-party security reports appears to be a fool's errand for organizations.

Bug bounties can be part of an overarching security posture, but the most important aspect is likely being prepared to respond to and fix vulnerabilities once they are identified rather than setting up a bug bounty program itself.

As exemplified by the case mentioned earlier regarding the difficulty in reporting the Facetime flaw to Apple, any enterprise maintaining software or delivering services to customers via technology has to think through a policy for receiving security disclosures and what the process looks like following the report. This should include an accessible, public communication method, routing the report to appropriate staff internally, and a guide for communicating back to a researcher on the vulnerability fix process. Organizations must also develop policies for requests for exclusions such as asking researchers not to do any unsolicited testing that would result in a denial of service (DoS), attempt at physical access, or anything that could be considered social engineering against an organization's employees.

Perhaps most important in creating such a policy is outlining expectations for working with third-party security researchers. The most common expectations of researchers after reporting a vulnerability all involved some form of communication – whether that's informing them when a fix is made, a timeline for a fix, or closer forms of collaboration such as fix validation. Perhaps, then, coordinated disclosure does not go far enough in its connotation in establishing software vendor responsibilities, and the next evolution of the disclosure debate needs to concentrate on a type of 'collaborative disclosure' in which vendors and independent security researchers expect to work in even closer concert with each other.

Appendix A: Demographics

Figure 8: Respondent regions

Source: 451 Research 2019 Collaborative Disclosure survey

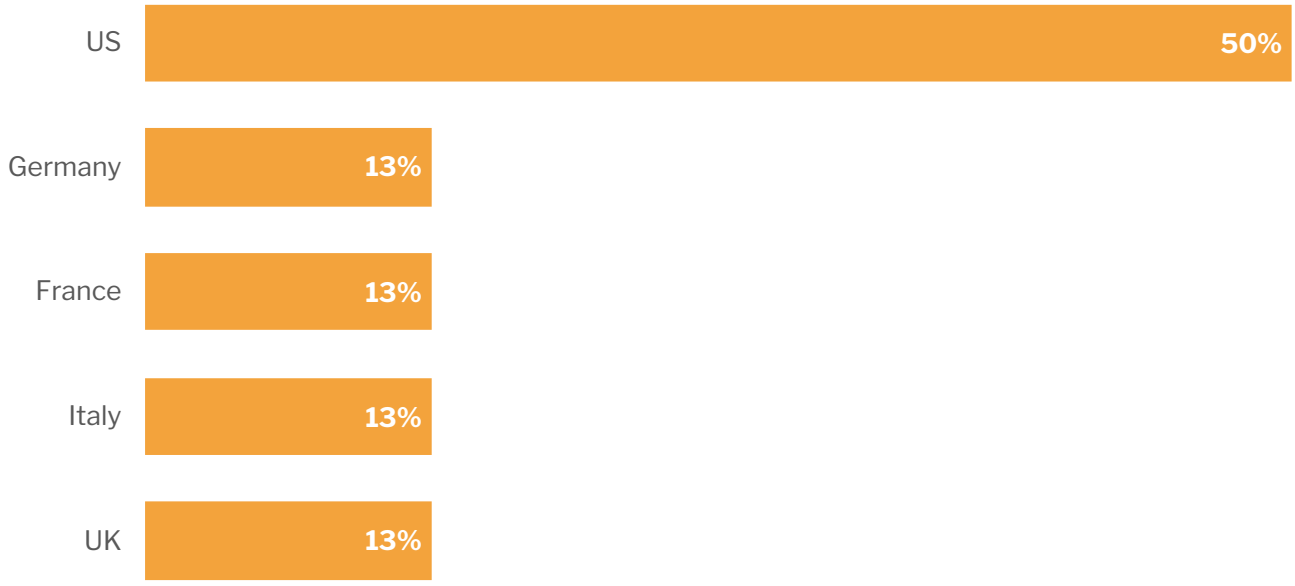


Figure 9: Number of employees in respondents' organizations

Source: 451 Research 2019 Collaborative Disclosure survey

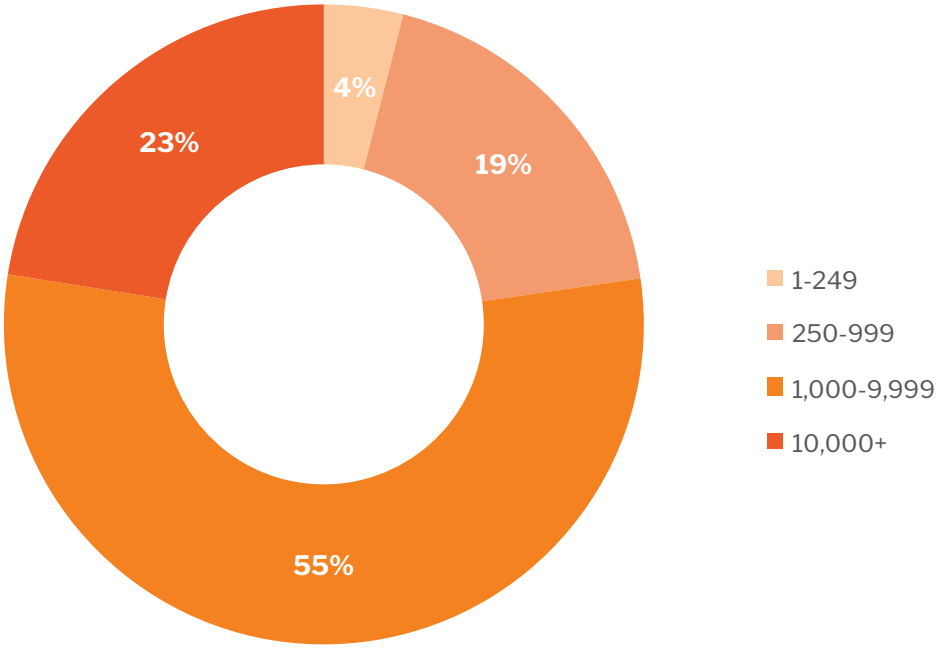


Figure 10: Industries

Source: 451 Research 2019 Collaborative Disclosure survey

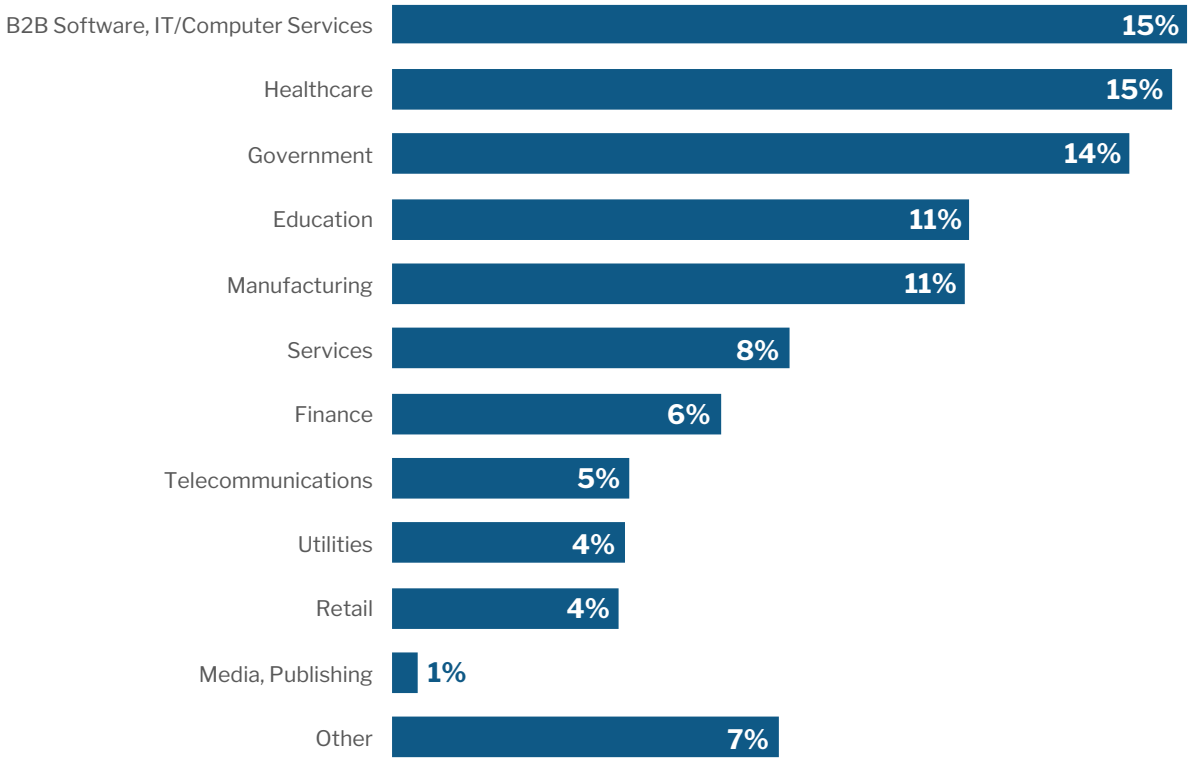
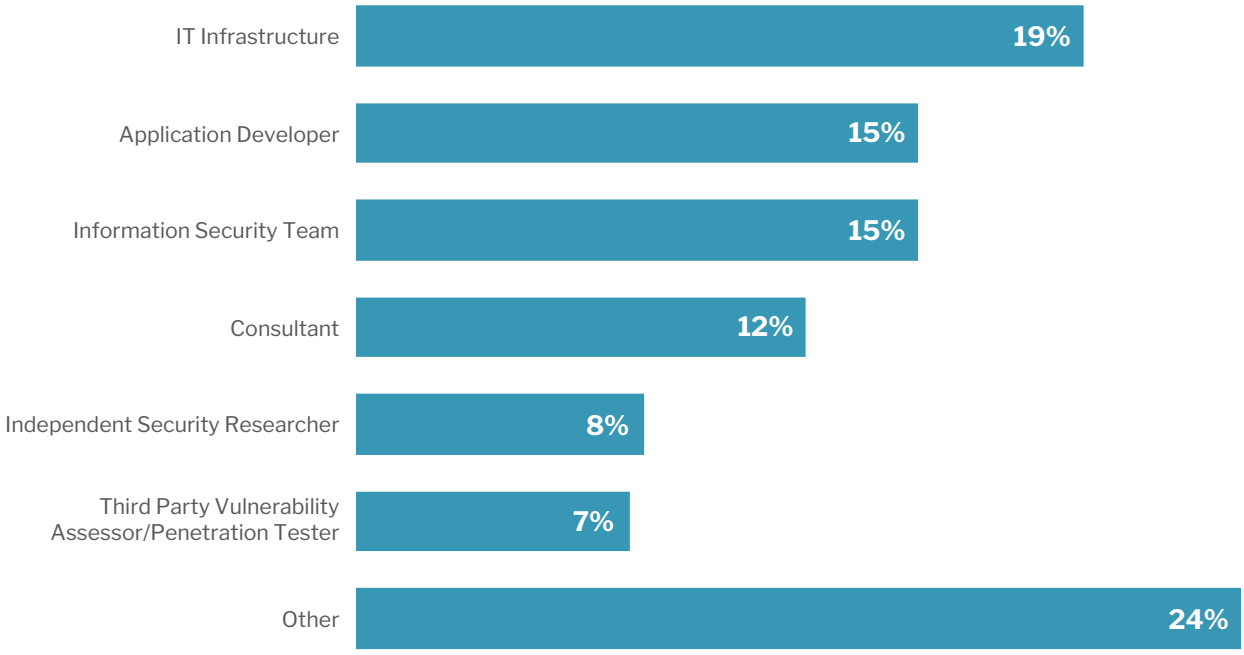


Figure 11: Job roles

Source: 451 Research 2019 Collaborative Disclosure survey



This may represent a significant opportunity to educate security researchers reporting vulnerabilities on the obstacles organizations face with fixing their flaws. Veracode's *State of Software Security Report Volume 9* revealed data that confirmed what many industry veterans recognize intuitively: it takes time to fix security flaws. That report, based on 700,000 application security scans by more than 2000 companies over a 12-month period, found that 70 percent of all flaws remained unfixed one month after discovery, and nearly 55 percent remained three months after discovery. Alarmingly, it also found that one in four high and very high severity flaws are not addressed within 290 days of discovery. This is not because developers are not interested in securing their code – rather, the sheer volume of vulnerabilities present in most organizations' application portfolios makes it necessary for them to make daily tradeoffs between security, practicality, and speed. There are just too many vulnerabilities for organizations to tackle at once, which means it requires smart prioritization to close the riskiest vulnerabilities first.

This may mean that some vulnerabilities linger after being reported by an outside security researcher not due to neglect or disregard for a vulnerability being reported, but because many organizations are doing a better job prioritizing by flaw severity. Still, Veracode data this year shows that organizations need to improve their effectiveness in weighing other risk factors in fixes such as the criticality of the application or exploitability of flaws.

Security researchers may hold unrealistic expectations regarding how flaws are being prioritized and fixed after being reported, making their own timelines to disclose publicly equally unrealistic and possibly unfair. Potentially, this is an area where organizations can better communicate how a reported flaw is being prioritized to reset those expectations with a researcher as part of enhanced collaboration.

With its combination of automation, process, and speed, Veracode becomes a seamless part of the software lifecycle, eliminating the friction that arises when security is detached from the development and deployment process. As a result, enterprises are able to fully realize the advantages of DevOps environments while ensuring secure code is synonymous with high-quality code.

Veracode serves more than 2,000 customers worldwide across a wide range of industries. The Veracode Platform has assessed more than 8 trillion lines of code and helped companies fix more than 36 million security flaws.

Learn more at *www.veracode.com*, on the Veracode *blog* and on *Twitter*.

Content Provided by

VERACODE

You change the world, we'll secure it.

Why We Commissioned This Research

Veracode envisions a world in which the software fueling economic growth and solving society's greatest challenges is developed secure from the start. As a leading provider of application security software, clients seek our advice and leadership around how to structure their teams, AppSec technology portfolio, and business processes to deliver the most secure software they possibly can. Our intent in commissioning this research was to establish a current view of perceptions around coordinated vulnerability disclosure and to define a set of clear recommendations that help businesses progressively deliver on the objective of developing software that is secure from the start.

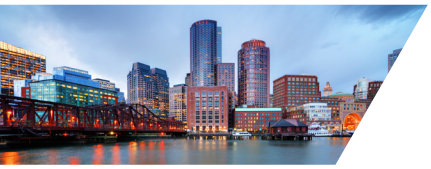
About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 1,000 client organizations globally through a combination of syndicated research and data, advisory and go-to-market services, and live events. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
1411 Broadway
New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
505 Montgomery,
Suite 1052
San Francisco, CA 94111
+1 212 505 3030

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 203 929 5700



BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

451 Research®