Cybersecurity Law Report
An Acuris company

cslawreport.com

September 25, 2019

VULNERABILITY TESTING

Vulnerability Disclosure Policies: A Cost-Effective Best Practice for Cybersecurity

By Marshall L. Miller and Adam Sowlati, *Wachtell Lipton Rosen & Katz*

The soaring frequency of data breaches and cyberattacks poses significant legal and reputational risks for any organization, elevating the importance of cybersecurity and cyber risk management. Increasingly, companies are viewing external security researchers, sometimes referred to as ethical hackers, as potential allies who can assist in early identification of system and product vulnerabilities. Technologically sophisticated organizations are implementing vulnerability disclosure policies (VDPs) to provide a framework for interacting with, and receiving reports from, third-party security researchers. While VDPs have not yet become the norm, they are increasingly being embraced by savvy corporations, regulators and thought leaders as a best practice. In this article, we provide an overview of the benefits of VDPs, outline the legal and regulatory landscape and highlight features of successful policies.

See "Capital One Breach Demonstrates Risk of Overlooking Vulnerabilities When Sending Data to the Cloud" (Aug. 14, 2019).

The VDP: A Key Vulnerability-Management Tool

A well-executed VDP enables an organization to harness the skills and expertise of the security researcher community to discover and remediate security vulnerabilities before they become a larger threat, result in a data breach or trigger a safety or public relations crisis. Organizations ranging from sophisticated companies to government agencies have implemented VDPs as a cost-effective way to improve overall security risk management, connecting with a global cadre of researchers to crowdsource the identification of vulnerabilities that internal engineers may have missed.

For example, within two years of launching its VDP, General Motors, an early VDP adopter, announced that it had worked with over 500 hackers to resolve more than 700 vulnerabilities across its supply chain. Many companies, including General Motors, utilize HackerOne, a vulnerability disclosure platform that hosts over 400,000 registered ethical hackers – an extensive security research network that, in 2018 alone, discovered over 100,000 vulnerabilities worldwide.[1] Most recently, it was through a VDP report from an external security researcher that Capital One first learned of the data breach of its servers, enabling the bank to shut down the vulnerability and work with law enforcement to identify the alleged culprit.

A VDP can encourage this sort of cooperation by providing researchers with a clear and reliable channel for communicating discovered vulnerabilities to an affected organization.[2] Without such a channel, researchers may simply choose to go public, exposing the organization to enhanced security threats, not to mention unfavorable public scrutiny – especially if a vulnerability were to expose consumer personal data or endanger public safety.

Moreover, VDPs can help dismantle a significant hurdle to generating helpful vulnerability reports: the chilling effect that stems from the fear of legal repercussions.[3] Under current law, ethical hackers engaging in vulnerability testing could risk liability under a number of statutes, such as the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act. Indeed, 60 percent of security researchers say they fear that "they may be subject to legal proceedings if they disclose their work."[4] And even the mere threat of legal action, such as a cease-and-desist letter, can silence security researchers and create a ripple effect of distrust in the researcher community.[5] Through a carefully crafted VDP, a company can help allay these concerns by providing a safe harbor from legal action for bona fide security researchers who submit reports in compliance with a VDP's terms.

See "How to Establish and Manage a Successful Bug Bounty Program" (Mar. 22, 2017).

VDPs As a Best Cybersecurity Practice

Increasingly, the market and government regulators expect companies to work with security researchers to protect critical systems and data assets, prioritize safety and mitigate risks. Implementing a VDP can provide compelling evidence to regulators, courts, investors and the public that a company is committed to cybersecurity best practices. There is reason for concern that failing to do so could expose a company to increased regulatory risk.

The Regulatory View: Case Studies From the FTC

In the United States, the Federal Trade Commission (FTC) has assumed a leading role in policing corporate cybersecurity practices, bringing scores of enforcement proceedings against companies for failing to maintain adequate cybersecurity programs in violation of Section 5 of the Federal Trade Commission Act (FTC Act).[6]

In comments before the Consumer Product Safety Commission, the FTC signaled its expectation that an effective cybersecurity program will include a VDP, stating that "the failure to maintain an adequate process for receiving and addressing security vulnerability reports from security researchers and academics is an unreasonable practice, in violation of Section 5 of the FTC Act." And in multiple enforcement proceedings, the FTC has cited the absence of a VDP as support for a finding that a company's cybersecurity program was inadequate.

In a 2014 enforcement proceeding, for example, the FTC found that an entertainment ticketing company's cybersecurity program violated the FTC Act in part because it did "not have a clearly publicized and effective channel for receiving security vulnerability reports." As a remedial measure, the FTC required the company to "establish and implement, and thereafter maintain, a comprehensive security program," which "at a minimum" should include "review, assessment, and response to third-party security vulnerability reports." In two other enforcement proceedings, the FTC similarly found that company cybersecurity programs violated the FTC Act and cited as a supporting factor the companies' failure to "implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents."[7]

The Broader Government View

Other government agencies in the United States have also embraced VDPs as a cybersecurity best practice. In the latest version of its influential Cybersecurity Framework, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) included VDPs as part of its Framework Core: "Processes [should be] established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (*e.g.* internal testing, security bulletins, or security researchers)." And in a report to the White House, the American Technology Council, working with the Department of Homeland Security, recommended: "At a bare minimum, agencies should establish vulnerability disclosure policies for at least their public-facing services, so that security researchers and other members of the public can report vulnerabilities they discover."

In 2016, the Department of Defense announced a limited-duration pilot program known as "Hack the Pentagon."[8] Under this program, DoD invited "qualified participants to conduct vulnerability identification and analysis on the department's public webpages." A few months later, DoD released the results of the program: Of the 1,400 hackers invited to participate, over 250 submitted a vulnerability report, "with 138 of those vulnerabilities determined to be legitimate, unique and eligible for a bounty."[9] Although the program cost the agency $150,000 in bug bounty payouts, Secretary Ashton Carter estimated that "the normal process of hiring an outside firm" to perform an equivalent security assessment would have cost "more than $1 million." Later the same year, DoD officially launched a Vulnerability Disclosure Program "aimed at improving the security of the Pentagon's unclassified, public-facing networks."[10] Although it no longer includes a bug bounty, the DoD's VDP allows "researchers to report bugs or flaws they discover in [DoD's] websites without fear of prosecution." Within eight months, the agency reportedly "fixed almost a thousand bugs."[11]

The Department of Justice has published guidance on the topic, documenting that "[a] n increasing number of organizations" are adopting VDPs to "improve their ability to detect security issues on their networks that could lead to the compromise of sensitive data and the disruption of services."[12] As a result, DOJ issued a framework to assist organizations in adopting VDPs, recommending that organizations "[d]raft a vulnerability disclosure policy that accurately and unambiguously captures the organization's intent," including explaining "the consequences of complying – and not complying – with the policy."[13] And at the 2017 Global Cyber Security Summit in London, Deputy Attorney General Rod J. Rosenstein advised that "[a]ll companies should consider promulgating a vulnerability disclosure policy," observing that the Defense Department's program "has been very successful in finding and solving problems before they turn into crises."

Other government agencies have followed suit. The Food and Drug Administration and Department of Homeland Security announced a Memorandum of Agreement between the two agencies related to the cybersecurity of medical devices, "most notably around coordination of vulnerability disclosures." The National Telecommunications and Information Administration released "Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure." And the National Highway Traffic Safety Administration published guidance for the automotive industry for "improving motor vehicle cybersecurity," expressing support for implementation of VDPs.

And it is not only the U.S. government that views VDPs as essential to cybersecurity; increasingly, international organizations and governments are emphasizing the importance of VDPs as well. For example, the International Organization for Standardization released ISO/IEC 29147:2018, which provides international guidelines for vulnerability disclosure, stating, "Vulnerability disclosure helps users protect their systems and data, prioritize defensive investments, and better assess risk." Moreover, the United Kingdom's National Cyber Security Centre has adopted a VDP, providing security researchers with a framework for reporting vulnerabilities found in U.K. government websites or systems.

Features of a Successful VDP

At its core, a VDP establishes a mechanism for third parties to report security vulnerabilities, a process for organizations to receive and address those reports, and a framework for the relationship between reporting researchers and receiving organizations. So, a rudimentary VDP can be as simple as a webpage with an email address for security researchers to report vulnerabilities securely, along with an intake and remediation process to address reported vulnerabilities. From there, VDPs can grow in complexity, tailored to the needs of a given organization. Many companies have found that expanding on the bare-bones version, and adopting a robust VDP with features like a safe harbor from legal action, can facilitate collaboration with the security researcher community.

Regular Communication

To begin, it is a best practice for a VDP to note the organization's commitment to working with the security researcher community to achieve greater security and safety. Many companies make a promise to stay in regular communication with participating researchers. This can include setting forth a time frame for responding to the researcher.[14] Here it is important that companies be realistic – it is far better to set an achievable time frame for responding than to blow past a self-imposed deadline and risk alienating the researcher.

Many security researchers seek recognition for their contributions. As a result, to drive participation, a number of companies, such as Twitter, have adopted mechanisms to generate publicity for researchers, such as online "halls of fame," which give credit to researchers who have submitted *bona fide* vulnerability reports.

See "How to Outsource Vulnerability Assessments to Hackers" (Oct. 25, 2017).

Defined Scope

VDPs should also provide clear notice to researchers as to the products and systems within the scope of the policy, in addition to any products and systems that are off-limits. A failure to set clear boundaries for a VDP can result in researchers engaging in vulnerability testing that could cause harm or foster ill will. The policy's scope will likely depend on "[t]he sensitivity of information stored or processed" on the system, or "[r]egulatory, contractual, or other restrictions placed on disclosure of protected classes of information,"[15] such as personal health data. A VDP can also prohibit certain techniques for discovering vulnerabilities that might adversely impact an organization's operations, such as "social engineering and denial-of-service attacks."[16]

Safe Harbor

Many companies also choose to offer security researchers a carrot in the form of a safe harbor from legal action – making a promise not to pursue civil claims or contact criminal authorities where security researchers work in good faith to comply with the terms of a VDP. By including a safe harbor that removes the specter of legal liability, an organization can incentivize researchers to report vulnerabilities. On the other side of the coin, some companies include a stick, expressly reserving the right to pursue legal action, where available, if researchers do not strictly comply with the terms and scope of a VDP. United is one example.

Monetary Award

Some companies, such as Google, go a step further by creating bug bounty programs, promising monetary awards to researchers who report actionable security vulnerabilities. At the Black Hat security conference this summer, for example, Apple promised awards of up to $1 million for reports of vulnerabilities in its iPhone operating system.[17] But beware that a bug bounty could result in a flurry of researcher activity, including potentially distracting reports of low-level or nonexistent bugs or possible attention from "black hat" hackers. A bug bounty program is most appropriate for an organization that has experience working with the researcher community and a mature process for triaging and resolving vulnerabilities.

See "WhiteHat Report on the Software Lifecycle and Visa Bug Bounty Program Demonstrate the Need for Greater App Security" (Nov. 7, 2018).

Handling of Vulnerability Reports

Although VDPs offer many benefits, companies can face legal and reputational risks if vulnerability reports are mishandled. Research has demonstrated that a lack of communication is one of the main reasons security researchers decide to share a vulnerability publicly.[18] For example, one company faced public backlash following a data breach when a security researcher revealed that he had alerted the company to the underlying website-related security issue eight months prior to the breach, but it had dismissed his report as a "likely scam."[19] Frustrated with the company response and tired of waiting for a fix, the researcher ultimately alerted the media. Shortly after the public disclosure, the company took its website offline to address the issue – but it was too late to limit the extent of the breach or avoid the reputational fallout. The company faced intense media scrutiny and allegations that it ignored a valid security report and allowed its website to leak customer data for eight months.[20]

This example highlights the importance of establishing a response protocol prior to publishing a VDP. Once a company invites security reports from third-party researchers, it must ensure that it regularly monitors the channels of communication and responds to reports within a reasonable timeframe. Otherwise, the company may frustrate the expectations of security researchers or, even worse, expose itself to expanded risk by failing to act upon a solicited vulnerability report before the vulnerability is exploited.

Beyond maintaining active communication with researchers, it is essential that organizations have the technical expertise and response capability to handle vulnerability reports. A failure to realize the technical significance of a vulnerability, for example, could have devastating consequences. Similarly, spending months or even weeks attempting to patch a vulnerability may not be an option if the vulnerability implicates product safety or exposes personal data. So before a VDP goes live, it is essential that an organization have a dedicated and experienced team ready to quickly examine and remediate any reported vulnerabilities.

Conclusion

An effective VDP is an increasingly important component of a robust cybersecurity program. As a bridge to the security researcher community, a VDP can enable an organization to significantly expand its security testing and vulnerability remediation capabilities at minimal cost. As a result, government agencies and security organizations increasingly view VDPs as a best practice, and the failure to have a VDP may even invite regulatory scrutiny or exacerbate potential liability. At the same time, a company should adopt a VDP only after a thoughtful planning process – one that ensures the company is ready to respond to incoming vulnerability reports. And a VDP should be tailored to a company's unique needs, with a calibrated scope and consideration given to whether to include more advanced features like a safe harbor or a bug bounty program. A carefully crafted VDP will send a strong message to researchers, customers, investors and regulators that an organization is committed to cutting-edge cybersecurity.

Marshall L. Miller is of counsel in the litigation department at Wachtell, Lipton, Rosen & Katz. His practice concentrates on advising corporations, board members and senior executives with respect to internal investigations, criminal defense, cybersecurity, data privacy, regulatory compliance and related civil litigation. Previously, he served as Principal Deputy Assistant Attorney General & Chief of Staff at the DOJ's Criminal Division. In that position, he supervised over 600 federal prosecutors and oversaw the Department of Justice's most significant prosecutions, including its FCPA practice and its flagship cybercrime unit.

Adam Sowlati is an associate in Wachtell's litigation department.

Lorraine L. Abdulahad, a student at Yale Law School who worked as a summer associate at Wachtell, co-wrote this article.

[1] *HackerOne Continues Growth With Record Bounties Awarded to Hackers in 2018 and Over 100,000 Valid Security Vulnerabilities Found for Customers*, HackerOne (Feb. 26, 2019).

[2] Nat'l Telecomm. and Info. Admin., Vulnerability Disclosure Attitudes and Actions (2015) [hereinafter NTIA Study].

[3] See Alexander Gamero-Garrido *et al.*, ACM Conference on Computer and Communications Security, Quantifying the Pressure of Legal Risks on Third-Party Vulnerability Research (Oct. 30–Nov. 3, 2017).

[4] *See* NTIA Study, *supra* note 2.

[5] *See, e.g.*, Kim Zeiter, *With Lock Research, Another Battle Brews in the War Over Security Holes*, Wired (May 6, 2015) (discussing "two aggressive legal letters" sent to security researchers who "attempted repeatedly to notify the company about problems with its product," and noting that the "letters have sparked outrage among some in the security community, which has long been at odds with companies that threaten legal action").

[6] 15 U.S.C. § 45. The Third Circuit upheld the FTC's authority in this area. See "In the Wyndham Case, the Third Circuit Gives the FTC a Green Light to Regulate Cybersecurity Practices" (Aug. 26, 2015).

[7] HTC America, FTC No. 1223049 (July 2, 2013); TRENDnet, Inc., FTC No. 1223090 (Feb. 7, 2014).

[8] *Statement by Pentagon Press Secretary Peter Cook on DoD's "Hack the Pentagon" Cybersecurity Initiative*, U.S. Dep't of Defense (Mar. 2, 2016).

[9] *Carter Announces 'Hack the Pentagon' Program Results*, U.S. Dep't of Defense (Jun. 17, 2016) (internal quotation marks omitted).

[10] Ellen Nakashima, *Hackers can now report bugs in Defense Dept. websites without fear of prosecution*, Wash. Post (Nov. 21, 2016).

[11] Tim Starks, *Tallying Fixes from the Pentagon's bug bounty program*, POLITICO (Aug. 7, 2017).

[12] U.S. Dep't of Justice, *A Framework for a Vulnerability Disclosure Program for Online Systems* (Jul. 2017).

[13] *Id.*

[14] *Department of Defense Vulnerability Disclosure Policy*.

[15] U.S. Dep't of Justice, *A Framework for a Vulnerability Disclosure Program for Online Systems* (Jul. 2017).

[16] *Id.*

[17] Thomas Brewster, *Apple Confirms $1 Million Reward For Anyone Who Can Hack An iPhone*, Forbes (Aug. 8, 2019).

[18] *See* NTIA Study, *supra* note 2.

[19] Dani Deahl, *Panera Bread leaked customer data on its website for eight months*, The Verge (Apr. 3, 2018).

[20] *Id.*