Cybersecurity & Data Privacy

STRATEGIC THINKING AND PRACTICAL LEGAL ADVICE

Five Questions General Counsels Should Ask about Vulnerability Disclosure

As businesses continue to leverage complex systems, managing the vulnerabilities inherent in such operations will become an increasingly important task. Vulnerabilities are the weaknesses in software code and network systems that render information and products susceptible to exploitation by malicious actors. As recent headlines attest, the consequences of such exploitation can be significant. Vulnerability management and the specific topic of vulnerability disclosure have thus become C-suite issues. Vulnerability disclosure is an essential aspect of how companies are managing the risks that vulnerabilities can pose. This article highlights five key questions that general counsels should consider as they evaluate whether vulnerability disclosure should serve as part of their holistic response to cybersecurity threats.

How Can Vulnerabilities Impact My Business?

Cybersecurity vulnerabilities can present serious legal, financial and reputational risks to companies. The vulnerabilities that pervade complex systems with millions of lines of code can impact both enterprise information technology networks and connected products. If such vulnerabilities are exploited, the real-world consequences can be significant. Vulnerabilities in the systems that support email servers or document databases can lead to the exposure or destruction of valuable intellectual property or ransomware attacks that freeze users out of these systems entirely. Vulnerabilities can also impact the increasingly ubiquitous Internet of Things. Connected devices are often difficult to both track and patch, rendering vulnerabilities in such products an unmitigated source of risk in the digital ecosystem. These vulnerabilities can impact a wide range of devices, from printers and routers to baby monitors and medical devices to modern vehicles and industrial machinery. Each category carries its own distinct risk profile. The results of successful exploitation can thus run the gamut from the exposure or destruction of personal data to direct physical harm to a large-scale distributed denial of service attack. These consequences could expose a business to government investigations, private litigation, loss of consumer confidence and extensive press coverage, all of which could potentially impact the organization's financial position.

What Is a Vulnerability Disclosure Program? How Is It Different Than a Bug Bounty Program?

A vulnerability disclosure program is a process by which an entity identifies, remediates and potentially discloses cybersecurity vulnerabilities to regulators or the public. These are often established with a focus on structuring possible engagement with third parties such as customers, private security researchers, the media and law enforcement concerning purported vulnerabilities. Such programs work to create a standardized process flow that identifies intake points for

vulnerabilities, key points of contact, roles and responsibilities for various stakeholders, and a path for escalation when necessary. Such programs are characterized based on a variety of factors including their scope, publicity, vendor engagement and size. One key factor in defining the nature of a program will be whether it employs bounties. Bounties are usually cash prizes awarded to researchers who identify and disclose vulnerabilities that are then validated by the organization. Vulnerability disclosure programs that offer bounties in exchange for vulnerabilities are often referred to as "bug bounty" programs. A vulnerability disclosure program can use bounties, but they are certainly not necessary to establish one.

What Are the Components of a Disclosure Program?

Every disclosure program is different and will be tailored to the specific threat profile, governance institutions and assets of a given company. But, in general, all vulnerability disclosure programs will share three primary elements. *First*, there will be a website or portal where the company or its vendor can receive vulnerability information directly from researchers. *Second*, there will be a back-end process flow that dictates how a given vulnerability will be validated and, if necessary, remediated. This will identify significant stakeholders and clarify roles and responsibilities at each stage of the process. *Third*, there will be an internal governance framework that supports the program and addresses issues related to change controls, management oversight, escalation procedures and guidelines for external communication.

How Can a Vulnerability Disclosure Program Help Manage Cyber Risk?

A vulnerability disclosure program is a tool that companies can use to mitigate the potential risks posed by vulnerabilities by supporting and enabling their disclosure and remediation *before* they are exploited. In essence, such a program is a way to break the cyber "kill chain" by identifying and fixing the very weaknesses that malicious actors use to attack systems and products. The benefits of such a program can be substantial. *First*, it can allow companies to improve their overall management of vulnerabilities in the systems they leverage and products they produce. Contributors to a program might discover problems that internal technicians might not have found until it was too late. *Second*, such a program can satisfy consumer expectations that companies move expeditiously and conscientiously to protect digital assets and respond to known risks in a reasonable manner. *Third*, a program can provide a structure for engagement with the security researcher community and thereby facilitate more streamlined and efficient identification of vulnerabilities. *Finally*, a vulnerability disclosure program also provides an opportunity to structure engagement with the US government and publicly demonstrate a commitment to responsible cybersecurity practices.

What Are the Applicable Regulatory Expectations?

Regulatory agencies are increasingly expecting companies to play an active role in managing vulnerabilities in their systems and products, including through the use of vulnerability disclosure programs. In recent years, a number of federal agencies have issued guidance on this topic. For example, the Federal Trade Commission recently "encouraged" companies to develop processes to manage and respond to vulnerability reports—the very purpose of a vulnerability disclosure program. The Department of Justice has also issued detailed guidance on how to institute a vulnerability disclosure program. And in addition to such trans-substantive guidance, industry-specific regulators have also publicized their own views on such programs. For example, the Food and Drug Administration has issued guidance stating that cyber risk management programs for medical devices—which are increasingly hardwired with Internet

connections—should incorporate "a coordinated vulnerability disclosure policy and practice." Likewise, the National Highway Traffic Safety Administration has highlighted the benefits of these programs in its guidance on cybersecurity best practices. As vulnerabilities and the impact of their exploitation continue to dominate headlines, regulators are likely to maintain their focus on the development and implementation of vulnerability disclosure programs.

For more information about the topics raised in this Q&A, please contact any of the following lawyers.

David Simon
+1 202 263 3388
dsimon@mayerbrown.com

Joshua Silverstein
+1 202 263 3208
jsilverstein@mayerbrown.com