ALSTON&BIRD

CYBER ALERT

A Publication of the Cybersecurity Preparedness & Response Team

ALSTONSECURITY.COM SEPTEMBER 15, 2016

Security Vulnerabilities: You Don't Need a Breach to Face Regulatory Scrutiny

By Kim Peretti, Lou Dennig and Jason Wool

Those who track newsworthy data breaches and other cybersecurity incidents know what type of fallout to expect from these events. Class action lawsuits from consumers, shareholders and financial institutions are now not an exception, but are increasingly becoming expected. Similarly, since the Federal Trade Commission (FTC) began focusing on data security nearly 15 years ago, it has engaged in enforcement actions against numerous companies that were subject to a data breach or other security compromise. State attorneys general have also joined the fray. Notably, these consequences are post hoc, in that they stem from the actual occurrence of a security incident that results in data compromise, loss or exposure. Recently, however, there has been an increase in regulatory and litigation actions based not on breaches or security incidents but on identified security vulnerabilities alone that, if exploited, could result in data compromise, leakage or exposure and so pose a potential *risk* of harm, whether economic or otherwise, to customers and consumers.

One possible explanation for this gradual change is that vulnerabilities are increasingly being brought to light through various means such as bug bounty programs, which are not only being adopted by more and more companies, but by a wider range of industries. Bug bounty programs (also referred to as vulnerability disclosure programs) provide incentives such as cash, airline miles or just recognition to security researchers who report vulnerabilities to companies. These programs are gaining increased legitimacy and publicity, underscored by Apple recently announcing that it would pay up to $200,000 for information on serious security vulnerabilities. According to a recent report, the number of companies with such programs has more than tripled year over year since 2013, with significant gains seen in the financial services, automotive, health care and retail sectors. U.S. government agencies are also increasingly encouraging their regulated entities to adopt vulnerability disclosure programs, with announcements in the first half of 2016 by the FDA, Department of Transportation and Commerce Department on this front.

In addition to identifying vulnerabilities through corporate-sponsored bug bounty programs, security researchers and hackers (with a wide range of motivations) frequently identify vulnerabilities and bring them to the attention of companies without such programs, sometimes with an expectation (or in some cases even a demand) that they receive a fee. After alerting known-impacted companies, they often publicly post information regarding vulnerabilities to spread awareness.

Regulator Scrutiny

One side effect of the rise in bug bounty programs, and disclosures by security researchers and others, is a commensurate increase in publicly known security vulnerabilities that can, in turn, lead to increased scrutiny from regulators (and the plaintiffs' bar) who become aware of the previously undisclosed vulnerabilities through these methods. For example, the FTC and FCC recently initiated parallel investigations into mobile device makers and carriers, prompted in part by an Android vulnerability known as "Stagefright" that became public after being reported to Google's bug bounty program last year. The vulnerability affected almost 1 billion Android devices and would have allowed attackers to remotely execute code merely by *sending* a text message to a device. Google paid the reporting security research firm $50,000 for their efforts, which allowed Google to develop and push out a patch.

In May, the FTC and FCC announced they had sent letters to several mobile device manufacturers (including Google) and mobile carriers seeking detailed information regarding, among other things, their "processes for reviewing and releasing security updates for mobile devices" and the "vulnerabilities that have affected those devices." The FCC specifically highlighted Stagefright in its press release announcing the inquiry. The FTC appears poised to continue considering enforcement actions related to security vulnerabilities—in response to the spate of ransomware attacks, FTC Chairwoman Edith Ramirez recently stated that a "company's unreasonable failure to patch vulnerabilities known to be exploited by ransomware might violate the FTC Act."

Several regulators have also been granted authority that would allow them to sanction companies before a vulnerability is ever exploited in the wild. The SEC's Office of Compliance Inspections and Examinations (OCIE), for instance, has initiated enforcement actions against a number of investment advisers, companies and broker-dealers for failing to have adequate written policies and procedures reasonably designed to protect customer records and information, as required under the Safeguards Rule of the Gramm–Leach–Bliley Act. For example, it recently penalized Craig Scott Capital for its employees' use of personal email addresses to conduct business involving sensitive customer data in contravention of the Safeguards Rule. While OCIE's enforcements have in some cases arisen from actual security incidents—as was the case in their most recent action against a major financial institution—in cases such as the one against Craig Scott Capital, OCIE has sanctioned companies merely based on the risk posed by certain conduct.

The Financial Industry Regulatory Authority (FINRA) operates under the same data security regulation as OCIE and has also engaged in enforcement actions against broker-dealers based solely on the risk posed by a particular practice. For instance, in one case in late 2015, FINRA sanctioned a member for, among other things, failing to have written supervisory procedures in place to ensure that customer information is "kept confidential, safeguarded, and encrypted prior to sending." The SEC's and FINRA's willingness to initiate actions where there is only a *risk* of harm due to inadequate policies is just a short logical step from bringing enforcement actions related to security vulnerabilities alone.

Other regulators have explicit legal authority to engage in enforcement actions based solely on a risk of harm. For example, the FTC is empowered to declare acts or practices in or affecting commerce to be unfair or deceptive. For the FTC to use its unfairness authority, the act or practice must cause or be *likely* to cause substantial injury to consumers (the Consumer Financial Protection Bureau (CFPB) operates with similar authority). In a recent enforcement action, the FTC used this authority to allege that HTC America "engaged in a number of practices that, taken together, failed to employ reasonable and appropriate security in the design and customization of the software on its mobile devices." These practices, in turn, allegedly "introduced numerous security vulnerabilities … which, if exploited, provide third-party applications with unauthorized access to sensitive information and sensitive device functionality." Notably, the FTC alleged that the vulnerabilities put consumers at risk of financial and physical injury and other harm.

The FTC has also used the deception prong of its authority to settle with companies that break promises (whether explicit or implicit) to engage in reasonable security practices based on unmitigated vulnerabilities. In one case, the FTC alleged that a company's iOS application failed to validate SSL certificates, giving rise to a vulnerability in the manner the application transmitted sensitive data. When a security researcher contacted the company about the issue, the report on the vulnerability was miscategorized and was not addressed until the FTC staff contacted the company. Accordingly, among other things, the FTC alleged that the company failed to provide reasonable and appropriate security by failing to appropriately test the application and maintain an adequate process for receiving and addressing vulnerability reports from third parties. The FTC further alleged that because an attacker could have intercepted sensitive data such as payment card information or login credentials transmitted from the application, that information could have, in turn, been misused and led to identity theft or other harms. Because the company had represented that they had reasonable and appropriate security in place, the FTC alleged it had made false and misleading representations in violation of Section 5 of the FTC Act.

Litigation from Identified Vulnerabilities

Regulators aren't the only entities leveraging security vulnerabilities to take legal action—the plaintiffs' bar has also sought to bring lawsuits based on vulnerabilities alone. Because of the Stagefright Android vulnerability, Samsung is now facing litigation in the Netherlands, where the half-million member Dutch Consumers' Association is alleging that the device maker engaged in unfair trade practices by failing to push out critical updates to its devices and providing inadequate information about vulnerabilities.

In the U.S., a plaintiffs' firm identified vulnerabilities at several law firms during a year-long investigation into law firm data security. Using the findings from its investigation, the firm filed a class action against an unnamed Chicago law firm seeking injunctive relief (that the firm fix the identified vulnerabilities) as well as damages under the theory that the firm's clients had been overpaying for services because part of their payments were allocated to keep the clients' data secure. The action was filed under seal, ensuring not only that the vulnerabilities were not made public (and so could not be exploited by hackers) but also that the identity of the defendant law firm remained confidential. Once the law firm patched the security vulnerabilities, though, the plaintiffs moved to unseal the complaint and publicly unveil the firm's identity, creating a potentially strong incentive for settlement.

This type of security vulnerability action is translatable beyond law firms to a broad range of entities, including SaaS/PaaS providers and any manufacturer whose products could be at risk due to a cyber attack, including Internet of Things and medical device manufacturers and automakers. This type of litigation, if successful, could create a monetary incentive for security researchers to partner with a plaintiffs' firm to bring similar actions and could create a tension between whether researchers identify vulnerabilities through bug bounty programs or the courts.

Another new avenue for security researchers to profit from identified vulnerabilities recently opened up: partnering with an investment firm to "short" the stock of the company with the vulnerability before publicly disclosing the issues. In late August, the security firm MedSec partnered with Muddy Waters Capital to release a report regarding vulnerabilities in cardiac care devices manufactured by St. Jude Medical. According to reports, Muddy Waters agreed to pay MedSec based on the degree to which the report caused the price of St. Jude's shares to fall—the deeper the decline, the more MedSec was paid. St. Jude's stock fell almost 5 percent shortly after the report was released. And soon after that, a patient filed a class action complaint against St. Jude using

the information from the MedSec report. For security researchers, this approach carries potential added risks—in response to the report, St. Jude filed a lawsuit against Muddy Waters and MedSec alleging, among other things, defamation, market manipulation and violations of a state deceptive trade practices act.

Practical Steps

In light of the growing trend of regulatory action and litigation resulting from the mere existence of cybersecurity vulnerabilities in products and services, and even from inadequate policies in corporate cybersecurity programs, companies may want to focus their efforts beyond just preventing actual data breaches and become more proactive in identifying and remediating vulnerabilities. Numerous regulators have emphasized the importance of conducting vulnerability assessments, including for software and other products being released to consumers. It is similarly important to have a formal system for addressing identified vulnerabilities.

Internal testing may also be supplemented by a bug bounty program or, at a minimum, a process for receiving, reviewing and, as necessary, remediating vulnerabilities reported by third parties. This can enable the company to remediate security vulnerabilities in a discreet manner and resolve issues before any potential litigation. Entities can also monitor and track vulnerabilities identified by security researchers in white papers or reported in the news, since not addressing those publicly known issues could lead to scrutiny from regulators. Lastly, companies should actively follow enforcement actions by the FTC and other pertinent regulators. By identifying any security vulnerabilities at similar companies leading to regulatory penalties, entities can assess their own organization for similar issues.

It is important to recognize that *not* looking for or ignoring vulnerabilities may make your company *more* vulnerable from a liability perspective. While in the past, personnel who caught wind of a potential vulnerability and were slow to address it (or chose to actively ignore it) may have escaped scrutiny, the current legal liability landscape increasingly demands active, and even proactive, engagement with vulnerability management.

If you have any questions or would like additional information, please contact Kimberly Peretti, Lou Dennig or Jason Wool.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, California, USA, 94303-2282 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333