The Legal Intelligencer

THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2016

PHILADELPHIA, TUESDAY, FEBRUARY 2, 2016

An ALM Publication

E-DISCOVERY AND CYBERSECURITY

Regulators Eye Medical Device, Consumer Cybersecurity for 2016

BY JANA LANDON

Maksim Kabakou/Fotolia

In the classic urban legend, a babysitter left alone in charge of sleeping children receives several mysterious, threatening telephone calls beckoning her to come upstairs. After two or three calls, she calls the operator (remember them?), who investigates, calls her back and tells her to get out of the house immediately. The police find a murderous lunatic just upstairs who was about to kill the babysitter.

Today, threats such as spear phishing, ransomware, and denial-of-service attacks are our modern-day, true urban legends. While there may not be murderous lunatics on the other end of every nefarious attack, the activities of the culprits impact thousands of individuals on a day-to-day basis. The Internet of Things has expanded in the past few years to include such things as fitness wearables, remote home security cameras, and "smart cars," giving enterprising cybercriminals new avenues into our data and our lives. During the summer of 2015, for example, security researchers demonstrated the ability to remotely do everything from unlocking doors and turning on windshield wipers to jerking steering wheels, disabling brakes and even paralyzing a Jeep on the highway. Home security cameras have also been prime targets for intrusions; one family in Rochester, Minnesota, found thousands of pictures of the interiors of homes around the world online that had been taken with Internet-enabled security cameras. Another report described a family member who heard someone talking through the security camera to his small child.

Both the U.S. Food and Drug Administration and the Federal Trade Commission have recognized that all of this new technology, meant to improve our lives, also comes with additional risks. To that end, both agencies have recently issued new guidance on how companies should be addressing cybersecurity in devices.

The FDA has had medical devices and cybersecurity on its mind for several years. Former Vice President Dick Cheney admitted in an interview with CBS's "60 Minutes" that he had the wireless capabilities of his pacemaker turned off in 2007. After he spoke to his doctor, they both agreed that the device could be used in a possible assassination attempt. This was later confirmed by master hacker Barnaby Jack in 2012; he had devised a way to hack into a wireless communications system that linked implanted pacemakers and defibrillators with bedside monitors that gather information about their operations.

The FDA issued its first guidance regarding cybersecurity and medical devices in 2013, focusing on medical devices and hospital networks. It stated that it had "become aware" of "cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations." These included medical devices and computers infected by malicious software, inadequate password protection, and a failure to update software. At that time, the FDA emphasized that it was being proactive and it knew of no breaches that compromised safety. It recommended that medical device companies take steps to limit unauthorized device access, develop strategies for protection and design fail-safe modes for critical functions, as well as provide methods for recovery of data in cases where security had been compromised. Similarly, in 2014, it issued guidance related to security standards in premarket submissions.

This past year, the FDA issued its first warning about a device that was vulnerable to attack. In May 2015, the FDA and the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team were made aware of cybersecurity vulnerabilities associated with Hospira's Symbiq Infusion System, a pump used to administer fluids such as insulin, pain relievers and chemotherapy drugs. Hospira and an independent researcher confirmed in July 2015 that Hospira's Symbiq Infusion System could be accessed remotely through a hospital's network. This could allow an unauthorized user to control the device and change the dosage the pump delivers, which could lead to over- or underinfusion of critical patient therapies.

In mid-January of this year, the FDA issued first-ever draft guidance on postmarket management of cybersecurity in medical devices. It outlined the steps medical device manufacturers must take to address cybersecurity risks, even after a device is approved. The draft guidance details the agency's recommendations for monitoring, identifying and addressing cybersecurity vulnerabilities in medical devices once they have entered the market. These include:

- Applying the 2014 National Institute of Standards and Technology voluntary Framework for Improving Critical Infrastructure Cybersecurity, which includes the core principles of identify, protect, detect, respond and recover.
- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk.
- Understanding, assessing and detecting the presence and impact of a vulnerability.
- Establishing and communicating processes for vulnerability intake and handling.
- Clearly defining essential clinical performance to develop mitigations that protect against, respond to and recover from the cybersecurity risk.
- Adopting a coordinated vulnerability disclosure policy and practice.
- Deploying mitigations that address cybersecurity risk early and prior to exploitation.

These guidelines demonstrate the FDA's renewed focus in this area; however, both the 2014 and proposed 2016 guidelines are in practice voluntary and nonbinding. Medical device vulnerabilities have been identified by several commentators as one of, if not the largest, cybersecurity threat of 2016, and one can see why—an enterprising hacker could easily hold one's life for ransom by compromising an insulin delivery system or pacemaker. Indeed, there is little that a consumer can do to protect himself or herself from these vulnerabilities—they must be managed by the device manufacturer.

Recent high-profile cases involving the FTC have reinforced the commission's ability to enforce privacy and cybersecurity standards on behalf of the consumer. Most notably, in *FTC v. Wyndham Worldwide*, 799 F.3d 236 (3rd Cir. Ct. App. 2015), the U.S. Court of Appeals for the Third Circuit affirmed that the FTC could use the prohibition on unfair practices in Section 5 of the FTC Act to challenge alleged data security lapses. This is good news for consumers, as the FTC clearly has the IoT in its sights. Earlier in 2015, the FTC issued "The Internet of Things: Privacy & Security in a Connected World," a report that outlines the FTC's best practices for navigating the IoT. It drew lessons from many of its privacy enforcement actions and created concrete recommendations for businesses interested in building devices. It also emphasized that there must be reasonable security requirements, that the amount of consumer data collected should be minimized, and that consumers should be given notice of what, exactly, is being collected and have the choice to participate in such collection.

The FTC also noted in a contemporaneous press release that it has a range of tools to protect American consumers' privacy related to the Internet of Things, including enforcement actions under laws such as the FTC Act, the Fair Credit Reporting Act and the Children's Online Privacy Protection Act; developing consumer education and business guidance; participation in multistakeholder efforts; and advocacy to other agencies.

The FDA and FTC's focus on the IoT is admirable; but, like most emerging areas, the extent of any cyberthreat will only be known after we have a major compromise of consumer data or patient health. Until then, consider your interaction with the IoT carefully. You never know when the next cyberhacking legend may involve one of your devices.

Jana Landon is counsel in Stradley Ronon Stevens & Young's Philadelphia office and founder and chair of the firm's e-discovery team. Her practice focuses on advising lawyers and clients on legal, technical and strategic issues regarding cybersecurity, electronic discovery and information governance, as well as representing clients in complex insurance coverage matters. She can be reached at jlandon@stradley.com or 215-564-8049.