KING & SPALDING

Client Alert

Data, Privacy & Security and FDA & Life Sciences Practice Groups

October 27, 2014

Medical Devices and Cybersecurity Risks
DHS investigates at-risk devices[1]

On October 2, 2014, the U.S. Food and Drug Administration (FDA) issued its final guidance on cybersecurity for medical device manufacturers, titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."[2] Less than three weeks later—after the recent surge in reported data breaches at several large corporations—media sources broke the story that the Department of Homeland Security (DHS) is investigating a different type of vulnerability: cybersecurity flaws in medical devices and hospital equipment. These flaws include security vulnerabilities that could lead to death or serious injury, as well as exposure to civil lawsuits or government investigations should such harms befall the public.

DHS's Investigation

According to media reports, the DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is investigating approximately two dozen potential security vulnerabilities in medical devices that may be exploitable by cyber criminals.[3] ICS-CERT began examining technical vulnerabilities in medical devices about two years ago, based on a cybersecurity researcher's concerns that networked medical devices were susceptible to malicious hacking. A DHS source was quoted saying that "[i]t isn't out of the realm of the possible" that medical device security vulnerabilities could "cause severe injury or death."[4]

Media sources report that ICS-CERT has identified software bugs and/or vulnerabilities in both infusion pumps and implantable heart devices. While no deaths or serious injuries resulting from cybersecurity vulnerabilities have yet been reported, DHS is concerned that malicious actors could exploit these bugs to gain control over the devices. In response to these concerns, ICS-CERT has been working proactively with medical device manufacturers to identify areas of exposure and mitigate risks before any medical devices or hospital equipment are attacked or protected health information or confidential data is stolen.[5]

Sources within DHS have apparently acknowledged that its probe is based in part on the research of Barnaby Jack, a recently deceased cybersecurity expert. Jack was well known for stating that he could hack into the

For more information, contact:

John C. Richter
+1 202 626 5617
jrichter@kslaw.com

Seth H. Lundy
+1 202 626 2924
slundy@kslaw.com

Christopher C. Burris
+1 404 572 4708
cburris@kslaw.com

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

John A. Drennan
+1 202 626 9605
jdrennan@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

wireless communications system that links implanted pacemakers and defibrillators with bedside monitors. Jack demonstrated a serious medical device cybersecurity vulnerability when, at a 2012 conference in Melbourne, he demonstrated that he could remotely cause an implanted pacemaker to deliver an 830-volt shock.[6] Similarly, Billy Rios, a private cybersecurity researcher, claims to have identified a bug in a popular implanted infusion pump, and to have developed a program that allows him to remotely control the pump and administer lethal doses of drugs to patients.[7]

Despite experts' assurances to patients with networked medical devices, at least one public figure—former Vice President Dick Cheney—has disabled some of the networking features of his implanted defibrillator, fearing that cyber terrorists could exploit those features. In response to questions about his decision to go off-line, Cheney explained that he was in a "relatively unique circumstance[]" as a former Vice President; however, others remain wary and some have even followed Cheney's lead in disabling network access on their medical devices.[8]

October 2, 2014 Final FDA "Nonbinding" Cybersecurity Guidance

The public notice of ICS-CERT's two-year investigation underscores the timeliness and relevance of the FDA's most recent guidance—issued October 2, 2014, at the start of Cybersecurity Awareness Month—to medical device manufacturers on cybersecurity, which is available **here**. The FDA guidance, consisting of "nonbinding recommendations" ostensibly modeled on the NIST Cybersecurity Framework, encourages manufacturers to develop controls to ensure the security of medical devices with the capability of connecting to the Internet, other devices, or other networks. For an in-depth discussion of the FDA guidance, please see the King & Spalding Client Alert available **here**.

The guidance encourages manufacturers to treat security measures as a fundamental part of the developmental process. It also acknowledges that device makers face challenges in striking the balance between implementing effective cybersecurity safeguards and ensuring that devices remain usable in their intended settings. Striking this balance is particularly important in the medical field, where physicians and other personnel often need to act with extreme urgency in emergency situations. The guidance sets forth examples of security functions for device manufacturers to consider, including limiting network access to the device through authentication protocols, implementing automatic timers to terminate sessions after a period of time, strengthening password protections, placing physical locks on devices, restricting software or firmware updates, and adding features that detect, log, and respond to security compromises.

The FDA also recommends including certain documentation as part of the premarket submission process to ensure implementation of appropriate cybersecurity controls. This documentation includes a hazard analysis, a summary of controls, and a "traceability matrix" that "links [] actual cybersecurity controls to the cybersecurity risks that were considered" by the manufacturer. Notably, on October 29, 2014, the FDA is holding a **webinar** on the Final Guidance called "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."

Our reliance on technology to safeguard some of our most important data—or, in the case of medical devices, to keep us alive—has led to an increase in the number of reported cyber attacks, the value of the data that has been compromised in these attacks, and the level of sophistication of cyber criminals. It is only a matter of time before malicious hackers target networked medical devices. Manufacturers can best prepare for, and react to, these attacks by considering the importance of cybersecurity in every step of the device development process, remaining vigilant to developing threats, and responding quickly to attacks.

* * *

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 30 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigations, e-discovery / e-disclosure, government investigations, government advocacy, insurance recovery, and public policy.

---

[1] The authors would like to express their gratitude to Amy Boring, Jimmy Michaels, and Alexander Pogozelski, associates in King & Spalding's Special Matters / Government Investigations Practice Group, for their assistance with this Client Alert.

[2] The FDA's *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* is available at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

[3] Jim Finkle, *U.S. Government Probes Medical Devices for Possible Cyber Flaws*, REUTERS (Oct. 22, 2014), *available at* http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022.

[4] *Feds Investigating Two Dozen Potential Hacks Targeting Life-Saving Medical Devices*, RT (Oct. 22, 2014), *available at* http://rt.com/usa/198320-medical-device-vulnerable-hackers/.

[5] Finkle, *supra*.

[6] Jeremy Kirk, *Pacemaker Hack Can Deliver Deadly 830-Volt Jolt*, COMPUTERWORLD (Oct. 17, 2012), *available at* http://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html

[7] Finkle, *supra*.

[8] *Id*.