Cybersecurity for Global Medical Device Supply Chain: The U.S. FDA's Role

Keman Huang, Sophie Herscovici, Stuart Madnick

Working Paper CISL# 2019-11

May 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Cybersecurity for Global Medical Device Supply Chain: The U.S. FDA's Role

Keman Huang, Sophie Herscovici, Stuart Madnick

Cybersecurity of medical devices is not only an issue of privacy, but a matter of life and death. The U.S. Food and Drug Administration (FDA) should increase its leadership role in managing emerging cybersecurity risks within the global medical device supply chain.

As a result of the growing use of information and communication technology (ICT) within medical devices, cybersecurity within medical devices is becoming a serious global issue that can no longer be ignored. Cybersecurity risks leave patients' lives vulnerable to cyber attack. Connection vulnerabilities could allow hackers to change the settings on a patient's St. Jude pacemaker remotely. Malware in MRI machines and CT scans could add or remove cancerous nodules, causing a patient to be misdiagnosed and wrongly treated. Ransomware attacks on hospitals could leave doctors and staff without the critical data they need to save patients' lives. Since medical devices rely on global supply chains and because cyber threats exist on an international level, it is crucial that the United States work with other countries to address medical device cybersecurity concerns.

The U.S. FDA's Efforts to Cyber Secure Medical Devices

The U.S. FDA is aware of the current vulnerabilities to medical devices and has begun to tackle these issues. Yet, the cybersecurity of medical devices is not exclusively handled by the FDA, but rather is under the purview of a collaborative network of government and private agencies. As shown in Figure 1, the FDA has partnered with the National Protection and Programs Directorate (NPPD) and the National Cybersecurity and Communications Integration Center (NCCIC), both of which are housed under the U.S. Department of Homeland Security (DHS). Both agencies help the FDA address medical device cybersecurity. The NCCIC supports the FDA by acting as a third party in assessing the cybersecurity risk of medical devices. The NPPD and FDA collaborate to enhance awareness of medical device cybersecurity vulnerabilities by providing alerts to healthcare stakeholders. In addition to their work with the DHS, the FDA works with healthcare delivery organizations (HDOs) and medical device manufacturers (MDMs) to ensure device cybersecurity. Both HDOs and MDMs are responsible for putting measures in place, like cybersecurity testing, to mitigate patient risk and ensure proper device performance. For example, the majority of hospital boards include cybersecurity as part of their risk management strategies, to mitigate risk independently of the FDA. In particular, HDOs are responsible for evaluating networking security and protecting hospital systems. For their pre-market submission, MDMs are required to submit documentation showing that their devices can detect and respond to cybersecurity incidents. In addition, they must also provide documentation to show that the device in question can recover from such incidents.

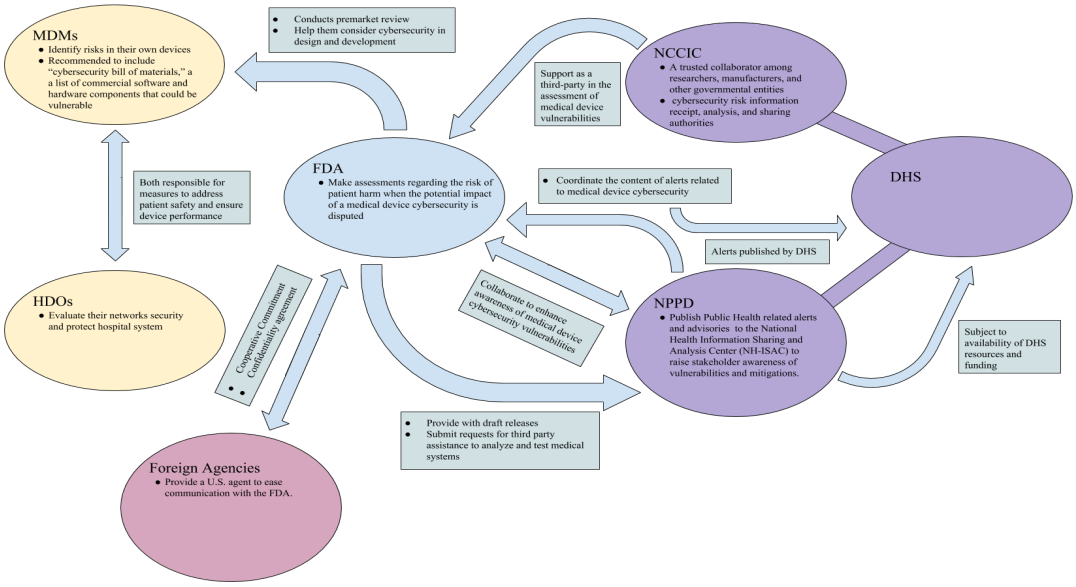

Figure 1: Cybersecurity collaborations between the FDA and other bureaucratic entities

From Medical Devices to the Global Medical Device Supply Chain

Beyond efforts to manage the cybersecurity risk within medical devices, it is of strategic interest for the FDA to reduce the systemic cybersecurity risks to the global medical device supply chain as a whole. This is because medical devices are not just designed and manufactured within the United States, but rather are part of a larger global supply chain. These efforts are all the more important given that cyber-attacks targeting supply chain vulnerabilities increased by 78 percent in 2018, as reported by Symantec in its 2019 Internet Security Threat Report.

The FDA requires MDMs to submit a cybersecurity bill of materials, which details the device parts or software components that are "off the shelf" (i.e. not developed by the manufacturer but directly purchased from third party suppliers). The FDA also works with MDMs to conduct pre-market development as well as to help them design and manufacture devices with cybersecurity in mind. Such public-private collaboration between the FDA and MDMs can help them work together to shape cybersecurity best practices for the medical device global supply chain.

On the international scene, the FDA is a leading member of the International Medical Device Regulators Forum (IMDRF), which brings stakeholders together to provide guidance on medical device regulation. Since cybersecurity is a relatively new, but pressing, issue in the realm of medical devices, the IMDRF recently added a new working committee to provide guidance on medical device security, led by Suzanne Schwartz of the FDA and Marc Lamoureux of Health Canada. Among many other things, the committee works to provide a technical document to inform stakeholders and promote cybersecurity information sharing. In addition, the FDA has presented at the forum on topics pertaining to cybersecurity, and other countries in the forum have adopted similar practices to manage their own cybersecurity. For example, like the

FDA, both Canada and the European Union have also adopted different classifications and standards based on the potential device risk to the patient.

These domestic and international cybersecurity commitments in medical devices place the U.S. FDA in a leadership position to push toward a more cyber secure global medical device supply chain. To achieve such a goal, the FDA should move forward beyond current efforts to more active approaches.

Toward a More Cyber Secure Global Medical Device Supply Chain

Despite current efforts, the FDA must take a step further and extend its responsibility to implement a cyber-related sanction mechanism, which will punish MDMs' risky cyber practices within medical device supply chains. While cybersecurity is mandatory for all medical devices, right now the FDA does not conduct pre-market cybersecurity testing for the devices. Instead, it has left it up to the MDMs. This practice is reasonable, as it would be impossible for the FDA to evaluate the cybersecurity risk for each and every medical device. However, instead of relying on the MDMs' report, FDA should build a more consistent system to report and track cybersecurity incidents on medical devices, instead of by coincidence. If a device experiences a cyber incident, the FDA should record the device, the date of the incident, and the issue that caused such threat etc. Once the MDM has fixed the vulnerability, the database could be updated.

Furthermore, the FDA should work together with the cybersecurity community to conduct random penetration tests of the medical devices to identify potential cybersecurity risks. The tests could look for potential vulnerabilities within the medical devices. Based on devices that experience cyber incidents, or fail to pass the tests, the FDA should develop a blacklist for high-risk MDMs and medical devices. Being blacklisted would limit the associated MDMs' capability to re-enter the market, such as a requirement to go through a much stricter cybersecurity evaluation during the pre-market submission process. In addition, in the same way side effects must be listed on medications, devices should list previous cybersecurity incidents. These sanction and deterrence mechanisms would incentivize manufacturers to truly consider cybersecurity and avoid incidents, in addition to making consumers aware of the risks associated with vulnerable devices.

Within the international landscape, the FDA should also further increase its responsibility for cybersecurity enhancement in the international medical device trade. Right now, the FDA uses the Confidentiality Commitment, a document providing a legal framework for the FDA to share information with a foreign organizations and to engage with foreign MDMs. The Cooperative Agreement is also used by the FDA to describe its willingness to cooperate with foreign governments and international companies. However, the FDA needs to move beyond these efforts and extend its international responsibility. The FDA should work closely with international trade agencies,

such as the United States Trade Representative (USTR), to develop trade policies directly related to medical devices based on their cybersecurity risk. For example, the medical devices imported from foreign MDMs that have historically provided highly cyber-risky devices should go through specific testing and auditing procedures. In addition, the FDA should further use its leadership role within the IMDRF to promote cybersecurity best practices within the global medical device supply chain, just as the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which provides a network for secure financial messaging services, uses its power to establish a baseline for its supply chains. Beyond offering guidance, the FDA should work together with IMDRF and international trade agencies, like the World Trade Organization, to extend IMDRF's responsibility and develop standardized, transparent, and trustful procedures for managing and harmonizing the cybersecurity policies for medical devices trading.

As more and more medical devices become electronic and linked to a network, there is a higher risk that these devices will be hacked. The FDA should continue its efforts to prioritize cybersecurity for medical devices. More importantly, the FDA should go further and use its power to become a leader in cyber securing the global medical device supply chain—a step which should include building deterrence mechanisms and extending its international trade responsibilities.

Authors' note: The research reported herein was supported, in part, by the MIT Internet Policy Research Initiative, which is funded by the Hewlett Foundation; Cybersecurity at MIT Sloan, which is funded by a consortium of organizations; and MIT Policy Lab at the Center for International Studies (MIT IPL).

Dr. Keman Huang is a Research Scientist at the MIT Sloan School of Management, where he works on cybersecurity management and policy, innovation ecosystems, and big data analysis. Sophie Herscovici is an MIT student studying economics, focusing on public policy. Professor Stuart Madnick is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management, Professor of Engineering Systems in the MIT School of Engineering, and Director of Cybersecurity at MIT Sloan (CAMS).