Published on *The National Law Review* https://natlawreview.com

Health Care Task Force Pre-Releases Report on Cybersecurity Days Before Ransomware Attack

Article By:

Dena Feldman

Christopher Hanson

Last week, the Health Care Industry Cybersecurity (HCIC) Task Force (the "Task Force") published a pre-release copy of its report on improving cybersecurity in the health care industry. The Task Force was established by Congress under the Cybersecurity Act of 2015. The Task Force is charged with addressing challenges in the health care industry "when securing and protecting itself against cybersecurity incidents, whether intentional or unintentional."

The Task Force released its report mere days before the first worldwide ransomware attack, commonly referred to as "WannaCry," which occurred on May 12. The malware is thought to have infected more than 300,000 computers in 150 jurisdictions to date. In the aftermath of the attack, the U.S. Department of Health and Human Services (HHS) sent a series of emails to the health care sector, including a statement that government officials had "received anecdotal notices of medical device ransomware infection." HHS warned that the health care sector should particularly focus on devices that connect to the Internet, run on Windows XP, or have not been recently patched. As in-house counsels understand, the ransomware attack raises a host of legal issues.

Timely, the HCIC report calls cybersecurity a "key public health concern that needs immediate and aggressive attention." The Task Force identifies six high-level imperatives, and for each imperative, offers several recommendations.

The imperatives are as follows:

1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity.

2. Increase the security and resilience of medical devices and health IT.

3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.

4. Increase health care industry readiness through improved cybersecurity awareness and education.

5. Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.

6. Improve information sharing of industry threats, weaknesses, and mitigations.

With respect to medical devices (imperative #2), the Task Force specifically advocates for greater transparency regarding third party software components. The report encourages manufacturers and developers to create a "bill of materials" that describes its components, as well as known risks to those components, to enable health care delivery organizations to move quickly to determine if their medical devices are vulnerable. Furthermore, the Task Force writes that product vendors should be transparent about their ability to provide IT support during the lifecycle of a medical device product. The Task Force also recommends that health care organizations ensure that their systems, policies, and processes account for the implementation of available updates and IT support for medical devices, such as providing patches for discovered vulnerabilities. The report suggests that government and industry "develop incentive recommendations to phase-out legacy and insecure health care technologies."

The Task Force also encourages medical device manufacturers to implement "security by design," including by making greater security risk management a priority throughout the product lifecycle, such as through adding greater testing or certification. In addition, the report encourages both developers and users to take actions that improve security access to information stored on devices, such as through multi-factor authentication. The Task Force recommends that government agencies, such as the U.S. Food and Drug Administration (FDA) and the Office of the National Coordinator for Health Information Technology (ONC) at HHS, consider using existing authorities to "catalyze and reinforce activities and action items" associated with this recommendation. This includes leveraging existing government guidance and industry standards, like FDA's premarket and postmarket cybersecurity guidance documents. Published in 2014 and 2016, these documents recommend that "manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of the [secure development lifecycle]." We have previously discussed these guidance documents here and here.

Finally, the Task Force recommends that the health care industry take a "long-range approach" to considering "viability, effectiveness, security, and maintainability of" medical devices. The Task Force states that each product should have a defined strategy and design that supports cybersecurity during each stage of the product's lifecycle. In particular, the Task Force encourages HHS to evaluate existing authorities to conduct cybersecurity surveillance of medical devices.

National Law Review, Volume VII, Number 139