HealthManagement
Promoting Management and Leadership

Improving Cybersecurity Through Public-Private Coordination

A unified effort by both the public and private sectors is critical to countering the growing cyber threats that are putting patient information and safety at risk, according to a report from the U.S. Health Care Industry Cybersecurity Task Force.

The report contains more than 100 recommendations to help increase cybersecurity across the healthcare industry. Theresa Meadows, co-chair of the task force, which was created by Congress through the Cybersecurity Act of 2015 to examine the sector's vulnerabilities, explains that the panel's intention was to provide actionable recommendations designed to increase security across the industry – each recommendation has one or more action items for implementing them.

"Real cases of identity theft, ransomware and targeted nation-state hacking prove that our healthcare data is vulnerable," states the report, which was finalised prior to the WannaCry ransomware attack that compromised more than 300,000 computers worldwide in at least 150 countries, including the National Health Service in the UK.

The task force's 100-plus recommendations are organised into six high-level imperatives, including increasing the security and resilience of medical devices and health IT. In particular, Meadows observes that medical devices are a "tough nut to crack because most institutions have medical devices for many years," adding that, on average, it's a 10- to 15-year investment timeframe.

"Our security posture has really changed over those 15 years, and those devices were not designed to have all of those mitigation factors in place, nor were they designed to be fully integrated to electronic health records," she points out. What's needed is to start replacing those legacy devices "so we can have them on the most current software and security without it being cost-prohibitive," she adds.

Another high-level healthcare cybersecurity imperative included in the report calls for improving information sharing of industry threats, weaknesses and mitigations. "Some organisations wouldn't want to report a security incident because of how it might affect them from a consumer standpoint, but there are a lot of good mechanisms to share critical information to fix and prevent issues without identifying the institutions that reported it," Meadows says.

According to Meadows, one of the strongest recommendations made by the task force is for the Department of Health and Human Services to create a cybersecurity leader role within HHS to align industry-facing efforts for healthcare cybersecurity. Currently many different programmes and agencies within and outside of HHS are responsible for cybersecurity, and Meadows says it's critical to have a single person who is responsible for coordinating these activities.

Overall, the successful implementation of these recommendations "will require adequate resources and coordination across the public and private sector," states the task force's report.

Source: Health Data Management
Image Credit: Pixabay

Published on : Mon, 12 Jun 2017