The Healthcare Sector is Strengthening its Cyber Health

National Cyber Security Awareness Month

October 1 - Since 2004, October has marked National Cyber Security Awareness Month for our nation. This is thus a good time for the healthcare sector to take stock and observe the progress we have made and the work we have ahead. As one of the sixteen critical infrastructures and one of the sectors that has traditionally lagged other sectors, we are working vigorously to catch up.

In February, an industry-wide, multi-stakeholder meeting was held to convene our industry around unity of effort to address our shared cybersecurity challenges. Leading up to and following that meeting, more than 200 organizations across the industry spectrum have stepped forward to join the Health Sector Coordinating Council's Cybersecurity Working Groups and its 13 Task Groups, all moving ahead with a likeminded cause – to strengthen our cybersecurity posture and ultimately protect patient safety and privacy. In June, HHS hosted the largest gathering to date of the HSCC Cybersecurity Working Group to take stock of our progress and sharpen our priorities.

Last year served as a wakeup call to our members and policymakers alike. Multiple global cyber-attacks (WannaCry, NotPetya and others) were launched – some of which affected our sector – and which delivered a devastating blow to our friends in the U.K. The National Health System was crippled for days as a result.

A landmark report was delivered to Congress in June 2017 by the Health Care Industry Cybersecurity Task Force, containing more than hundred recommendations to strengthen our sector's posture.

Together, these activities served to galvanize our industry on the recognition and commitment that coordination is the key to combatting these threats.

And coordinating we are. Since the start of 2018 each of our workgroups is tackling multiple recommendations laid out by the Task Force. We have launched a website for the industry to serve as a resource, and we have advocated to the Centers for Medicare & Medicaid Services (CMS) for a Stark exception to permit donations of cybersecurity technology and resources to assist those healthcare providers who need more help strengthening their posture. And we have engaged with DHS to enhance that partnership and gain awareness of the many cyber resilience services they provide to critical sectors like ours

We also have multiple work products in the pipeline. Specifically, we plan on releasing soon: 1) voluntary best practices intended for manufacturers to increase the security and resilience of medical devices; 2) voluntary best practices aimed at healthcare providers of various sizes intended to improve their security posture; and 3) a voluntary curriculum which can be used by medical schools to train clinicians on how to manage their use of information technology, electronic health records, and medical devices in a secure and responsible way.

Working with our federal partners is also pivotal to our industry's success. To that end, momentum continues to mount with policymakers both within the Administration and Congress to address cybersecurity threats, and healthcare is garnering more attention. This is evidenced by:

- The National Cyber Strategy released last month, which said the federal government will work with the private sector to manage risks to critical infrastructure at the greatest risk, including healthcare.
- House passage of the reauthorization of the Pandemic and All-Hazards Preparedness and Advancing Innovation Act of 2018 (H.R. 6378) which contains for the first time cybersecurity provisions and requires the U.S. Department of Health & Human Services (HHS) to submit to Congress a strategy for public health preparedness and response to address cybersecurity threats.
- An upcoming joint table-top exercise with HHS to respond to a blended incident involving a pandemic flu and a cascading ransomware cyber-attack.

We recognize that patient safety has taken on a new dimension that demands our attention – the recognition that patient security requires cyber security. The health sector is now organized and working to fortify the industry's immune system against a cyber epidemic that has become as infectious as a human epidemic.

If you are a healthcare organization and interested in getting involved in our mission, please contact us at https://healthsectorcouncil.org/contact/