WHA WISCONSIN HOSPITAL ASSOCIATION
ADVOCATE. ADVANCE. LEAD.
The Valued Voice

Vol. 68, Issue 26 Thursday, June 27, 2024

Health Care Emergency Readiness Planning: Cybersecurity Planning Resources Available

The threat of cyber security breaches in the U.S. health care system seems to only rise every year. Recent high-profile cyber-attacks on entities such as Change Healthcare, HSHS and Ascension have shown just how significant the impacts of cyber-attacks can be.

WHA just concluded its annual Wisconsin Rural Health Conference in Appleton, including a presentation by M3 Insurance and Ghostscale entitled *The Rise of Smart Threats: How AI is Changing Ransomware and Social Engineering.* The presentation, attended by almost 300 Wisconsin hospital leaders, focused on how artificial intelligence is changing the threat landscape in the health care space, including how it may allow relatively unsophisticated bad actors to create social engineering and ransomware schemes that can cripple large organizations. The presentation outlined strategies hospitals can implement to reduce vulnerabilities to such attacks.

Representatives from M3 Insurance and Ghostscale give a presentation on "The Rise of Smart Threats" at the Wisconsin Rural Health Conference, June 21, 2024.

For hospital leaders and emergency planning coordinators looking for more information and resources on cybersecurity, ASPRTRACIE and HHS have a variety of resources available to assist with planning for and preventing health care cyber-attacks. This includes a recent webinar series on Cybersecurity Incident Response Preparedness from the Health Sector Cybersecurity Coordination Center (HC3). This webinar contains updated information on current top threat actors and recommendations, as well as resources for executing planning exercises.

The HC3 also has a cybersecurity video on-demand series that includes training videos for health care organizations as well as a 2024-2029 strategic plan for addressing the operational, technological and governance challenges posed by significant health care industry trends over the next five years. The HC3 is a respected collaborative that includes Wisconsin health system members Ascension, Froedtert Health, HSHS, Gundersen Health and Mayo Clinic, as well as health records organization Epic Systems Corporation and WHA's Information Center (WHAIC).

In partnership with the HC3, the 405D Program is a collaborative effort between the Health Sector Coordinating Council and the federal government to align health care industry security practices. It has a Knowledge on Demand learning center that includes easy-to-digest video series on cyber threats. It has also prepared an extensive report aligned with other federal agency and partner efforts entitled Hospital Cyber Resiliency Initiative Landscape Analysis. This comprehensive document includes health industry cybersecurity practices specifically tailored to hospitals.

Among its key findings are that the health sector continues to be a top threat due to a constantly evolving threat landscape that occurs due to changes and innovations in care delivery, continued fissures in the health care supply chain and antiquated hardware and software utilized by some hospitals. Directly targeted ransomware attacks have been a growing threat despite hospitals reporting measurable progress on security frameworks for email systems. This has led to a continued rise in cybersecurity insurance

premiums. Five of 56 hospitals surveyed in 2022 experienced increases of more than 100% in these premiums, whereas 32 experienced increases just below 35%. Yet, the report found a strong correlation between those who have adopted strong health industry cybersecurity practices and cybersecurity resiliency.

Contact WHA Vice President of Federal and State Relations Jon Hoelter with questions.

Other Articles in this Issue

- 2024 Wisconsin Rural Health Conference in the Books
- Wisconsin Hospitals State PAC & Conduit Surpasses $200,000, Heads into Second Half of 2024 Fundraising Campaign
- Health Care Emergency Readiness Planning: Cybersecurity Planning Resources Available