Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Building a Stronger Healthcare Workforce for Cybersecurity

National Cyber Security Awareness Month

October 24 - As National Cyber Security Awareness Month moves into its final week in October, it is important to note that the healthcare sector – both industry and government - is stepping up to address accelerating cybersecurity threats affecting healthcare operations, data, and patient safety.

In June 2017 the Health Care Industry Cybersecurity (HCIC) Task Force report described healthcare cybersecurity as being in critical condition and listed the need to "develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities" as one of six high level imperatives for action.

The HCIC recommendations include: 1) Identifying the cybersecurity leadership role for driving robust policies, processes and functions with clear engagement from executives, 2) Establishing a model for resourcing the cybersecurity workforce with qualified individuals, 3) Creating Managed Security Service Provider models to support small and medium-sized health care providers, 4) Guiding small and medium-sized providers toward options for migrating patient records and legacy systems to secure environments.

A significant portion of medium and small health providers don't consider information technology a strategic asset towards the system's success. In this light, and considering cybersecurity being a sub-component of IT, cybersecurity is then an afterthought. The security program is an additional duty, and secondary priority, for IT staff already burdened with full time jobs. To adequately prepare for and mitigate the cyber threats facing healthcare, health providers must select appropriate cybersecurity leadership and enable their efforts for an enterprise-wide strategy to protect patient lives and data.

It is clear that health organizations must be creative and flexible in finding the appropriate leadership and staff, with appropriate skills, at the right price. The Health Sector Coordinating Council is developing a white paper soon to be published that will offer ideas for how organizations can improve their capabilities for managing cybersecurity risk with deeper cybersecurity bench strength in their workforce. For example:

Student Staffing Pipeline: Students develop cybersecurity skills with part-time work or externship work while attending school. The goal doesn't stop at hiring students. The organization must turn them into effective members of the cybersecurity mission, allowing them to perform work in a way that they are not viewed simply as "students" by the organization—but viewed as cybersecurity analysts.

Clinical Engineering staff to Cybersecurity: Map the convergence of work efforts that clinical engineering and biomedical staff members are performing that were traditionally information technology and security competencies. The security of medical devices as patient safety and patient security concerns have brought clinical engineers and biomedical team personnel closer to cybersecurity professionals. Cybersecurity teams will benefit where these conversions can be made.

IT Staff Conversion to Cybersecurity: Develop a plan of success for IT professionals to make the transition from traditional IT roles to cybersecurity roles, including mentoring, educational support, and outreach.

Cybersecurity Staff Professional Development and Retention: Enhance skillset of existing cybersecurity staff to augment program capabilities. Enable greater individual professional growth and support with education, mentoring programs, and outreach.

Outsourcing Cybersecurity: Compensate for deficiencies regarding specific skillsets and/or need for 24x7 staffing. Not all organizations have reached a point of maturity for a fully functional and staffed organization. Some locations may have difficulty recruiting and retaining particular disciplines. For example, finding experts in the Governance, Risk, and Compliance (GRC) discipline, the ability to fully staff a 365x7 Security Operations Center (SOC), or a full-time need for penetration testers, presents challenges for some organizations in terms of recruiting and/or retaining the right people they can also afford.

The healthcare sector is working hard to get ahead of the threats facing the sector and its patient population in partnership with government and critical healthcare subsectors like direct patient care, health IT, medical devices, pharmaceuticals and health plans and insurance. Cybersecurity in the healthcare sector isn't just an IT security problem, or a regulatory compliance problem, but one that needs the holistic treatment of health providers, chief medical officers, CIO's, general counsels, and the C-suite in general. In this way we can collaboratively diagnose our cyber health, prescribe a regimen of treatment and move us closer to inoculation against an epidemic of cyber vulnerability.

##