Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

Protecting Critical Healthcare Innovation Capital From Cyber Theft

By Omar Tisza
Health Sector Coordinating Council

October 28 – Everyday, healthcare organizations – from the neighborhood physician practice to the multibillion dollar pharmaceutical – are hit with cyberattacks that threaten the integrity of healthcare critical infrastructure and healthcare delivery. There is no shortage of ransomware news headlines; but insight into the theft of innovation capital (IC), by comparison, is difficult to come across in the public sphere and even among healthcare cybersecurity practitioners.

IC is not only defined as traditional intellectual property, but as the broader umbrella of sensitive and proprietary data encompassing trade secrets, derived insights, process controls, specific data methods, and more. As we continue celebrating National Cyber Security Awareness Month (NCSAM) and drawing parallels between the human system, the healthcare cybersecurity landscape, and the threats that impact the health sector, the theft of IC is like a silent disease that goes unnoticed until it takes a debilitating toll on the human body.

While the effects from IC theft are difficult to identify and quantify, the economic and financial damage can have severe impacts on affected organizations, and the entire health sector by extension. To mitigate the risk of IC theft, healthcare organizations must triage their risk scenario in a manner that *actively* prevents IC loss. The effective implementation of policy and governance-based measures (which are generally considered more *passive* in their protections) in tandem with aggressive cybersecurity control is an ideal path to preventing the loss of IC. The damage incurred by losing IC, even if recovered from a threat actor, is monumental and potentially costing organizations a crippling number of resources that may necessitate scaling back goods or services, or even limiting the ability of an organization to fund future innovations.

When compared to non-IC data, the inherent value of IC is vital for the national security and economic prosperity of the nation, and part of an industry-wide issue. While each organization is responsible for protecting their own IC, the interconnected and web-enabled systems supporting enterprise operations necessitate a public-private approach, with robust bi-lateral collaboration and information sharing at a minimum. The healthcare private and public sectors, and the United States, are uniquely positioned to address the loss of IC and implement effective and sustainable measures.

Implementing strategies for adequate IC protection have become an imperative. The sustainability of IC protection depends upon the data identification and protection of IC, and the infrastructure – including workforce – needed to operationalize, maintain, and improve the state of protection with the necessary controls. In the short term, however, there are bite-size steps we can take to catalyze systemic change. Changing the tendency to dis-incentivize the disclosure IC theft incidents (and any lessons learned among both public and private stakeholders) can move the needle towards an ideal IC protection model. Naturally, matters related to IC, including an IC loss incident, can be highly sensitive for both the public and private partners involved. But, the evolution of an IC security posture must center around sharing information and lessons learned for continuous improvement, and eventually aim towards building a comprehensive national and international effort to address IC loss from both policy and operational angles, with the United States positioned as the leader of such an effort.
To cure the illnesses of the health sector, and address the theft of IC, a silent and debilitating condition; the Health Sector Coordinating Council Joint Cybersecurity Working Group is currently finalizing a best practices document focused on recommendations for protecting IC (releasing in early 2020) to continue upholding patient safety, cyber safety, and the inoculation of our cyber immune system against tough illnesses and the ever-shifting cybersecurity threat landscape.

Omar Tisza is the Business Operations Coordinator for the HSCC Joint Cybersecurity Working Group