Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Health Industry Publishes Cybersecurity Best Practices for Protecting Innovation Capital

Washington, D.C., May 14, 2020 - The Healthcare and Public Health Sector Coordinating Council (HSCC) today released a white paper providing guidance for how healthcare organizations can protect trade secrets, medical research and other innovation capital from cyber theft.

The Health Industry Cybersecurity Protection of Innovation Capital (HIC-PIC) guide, developed by the HSCC Joint Cybersecurity Working Group, examines U.S. and international legal remediation trends for innovation capital (IC) protection, outlines enforcement challenges, and provides a range of specific information protection control recommendations to improve healthcare IC protection overall. Case studies highlight factors that enable IC theft, capabilities for detecting and defending against IC theft, and the significant business consequences resulting from each loss.

The HIC-PIC also implements a major recommendation in a 2017 report by the Health Care Industry Cybersecurity (HCIC) Task Force, to "Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure." The HCIC Task Force was appointed and co-led by the U.S. Department of Health and Human Services and industry executives pursuant to the Cybersecurity Act of 2015, and has been a guiding reference for the HSCC to address cybersecurity challenges facing the health sector.

"Recent indications of attempts at industrial espionage to steal vaccine data and other medical research make the HIC-PIC guide a particularly timely resource for the health sector," said Russell Koste, Chief Information Security Officer of Alexion Pharmaceuticals, Inc., and a co-chair of the HSCC task group that produced the report.

"At the same time," Koste continued, "the COVID-19 pandemic appears to have heightened barriers to trade which can impose an adverse effect on international trade relations and the industry's ability to protect IC."

Greg Garcia, Executive Director of the HSCC Cybersecurity Working Group, added: "Whether we are operating in extraordinary situations like the global pandemic or business as usual, robust IC protection controls must remain top of mind to enable secure data and technology transfer in the supply chain, which safeguard domestic innovation and mitigate the risk of IC loss to threat actors."

The HIC-PIC guide is the 3rd HSCC cybersecurity publication for the health sector in 2020, and the 8th in the last 18 months. These guidance documents and best practices are intended to assist the health sector to improve the security and resiliency of its operations and data, for the benefit of patient safety and public health. The next publication, to be released the week of May 18, will provide guidance for tactical crisis response to COVID related cyber threats.

Other HSCC Joint Cybersecurity Working Group resources published in 2019 and 2020 include:

1. Information Sharing Best Practices: Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP)
2. Management Checklist for Teleworking Surge During COVID-19 Response: https://healthsectorcouncil.org/covid-checklist/
3. Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM): https://healthsectorcouncil.org/hic-scrim/
4. Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO): https://healthsectorcouncil.org/hic-miso/
5. Health Industry Cybersecurity Workforce Development Guide: https://healthsectorcouncil.org/workforce-guide/
6. Health Industry Cybersecurity Practices (HICP): https://healthsectorcouncil.org/hhs-and-hscc-release-voluntary-cybersecurity-practices-for-the-health-industry/
7. Medical Device Joint Security Plan: https://healthsectorcouncil.org/the-joint-security-plan/

About the Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group (JCWG). The HSCC is an industry-driven public private partnership of health companies and providers developing collaborative solutions to mitigate threats to critical healthcare infrastructure. It is one of 17 designated critical infrastructure sectors organized to partner with the government under Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience. The HSCC Joint Cybersecurity Working Group (JCWG) includes more than 260 medical device and health IT companies, direct patient care entities, plans and payers, labs, blood and pharmaceutical companies, and government partners working together to develop recommendations and best practices to strengthen the security and resiliency of the sector against evolving cybersecurity threats and vulnerabilities for the ultimate benefit to patient safety and public health.

For more information: Greg Garcia, HSCC Cybersecurity Working Group Executive Director: Greg.Garcia@HealthSectorCouncil.org or visit us online at https://healthsectorcouncil.org

##