Health Industry Publishes
Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)

Washington, D.C., May 18, 2020 - The Health Sector Coordinating Council (HSCC) and the Health Information Sharing and Analysis Center (H-ISAC), today jointly released a tactical guide for how healthcare organizations can manage cybersecurity threats that occur during a crisis such as the COVID-19 pandemic.

The Health Industry Cybersecurity Tactical Crisis Response (HIC-TCR) Guide is constructed to advise health providers on tactical response activities for managing the cybersecurity threats that can occur during an emergency. Smaller organizations can leverage this document as a list of activities to consider. Larger organizations can use it as a sanity check for existing plans.

The HIC-TCR also implements a major recommendation in a 2017 report by the Health Care Industry Cybersecurity (HCIC) Task Force, that "Industry should implement cybersecurity incident response plans, which are reviewed and tested annually." 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.

"During a crisis, technology, processes and even the way we work can change on a dime; this opens up brand new attack surfaces, and the vulnerability from malicious cyber-attacks increases as well," said Erik Decker, Chief Information Security and Privacy Officer of University of Chicago Medicine and a co-lead of the task group that produced the report. "To thwart these attacks before they occur, it is essential for health care organizations to analyze, establish, implement, and maintain cybersecurity practices that are responsive to the crisis at hand."

Denise Anderson, President of the Health Information Sharing and Analysis Center and the task group co-lead, added, "The HIC-TCR was developed by a team of seasoned practitioners in healthcare who have offered their experience and expertise in cybersecurity incident response to provide other healthcare organizations with a roadmap of important things to consider when either developing or refining an incident tactical response plan. While every plan has to adapt to the needs of each situation and each organization, there are solid basic best principles that should be adopted, and this guide is a great tool to use."

The HIC-TCR guide is the 4th HSCC cybersecurity publication for the health sector in 2020, and the 9th 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 publications to be released are cyber and physical security guidance for returning to work as COVID-19 quarantines wind down and an expansion of the 2019 publication for Supply Chain Cybersecurity Risk Management.

Other HSCC Joint Cybersecurity Working Group resources published in 2019 and 2020 for sector-wide benefit include:

1. Protecting Innovation Capital from Cyber Theft: Health Industry Cybersecurity Protection of Innovation Capital (HIC-PIC)
2. Information Sharing Best Practices: Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP)
3. Management Checklist for Teleworking Surge During COVID-19 Response: https://healthsectorcouncil.org/covid-checklist/
4. Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM): https://healthsectorcouncil.org/hic-scrim/
5. Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO): https://healthsectorcouncil.org/hic-miso/
6. Health Industry Cybersecurity Workforce Development Guide: https://healthsectorcouncil.org/workforce-guide/
7. Health Industry Cybersecurity Practices (HICP): https://healthsectorcouncil.org/hhs-and-hscc-release-voluntary-cybersecurity-practices-for-the-health-industry/
8. 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.

The HIC-TCR document can be downloaded at https://HealthSectorCouncil.org/hic-tcr

For more information:

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

H-ISAC: Contact@H-ISAC.org or visit us online at https://h-isac.org/

##