American Hospital Association™

Advancing Health in America

Cyber Alert

**January 6, 2020**

# Hospitals and Health Systems Should be Vigilant for Potential Cyberattacks from Iran, Middle East

***Now is the time to assess your organization's cybersecurity posture***

A U.S.-led airstrike Jan. 3 in Iraq eliminated Qassem Soleimani, the head of the Iranian Revolutionary Guard Corps (IRGC)-Quds Force, a U.S.-designated Foreign Terrorist Organization. Although the U.S. government has not identified a specific threat from Iran targeting U.S. health care, the public has been asked to remain vigilant for physical and cyber-based suspicious activity.

Many in the U.S. government believe that Iran will attempt a retaliatory strike against U.S. interests overseas or potentially against U.S. critical infrastructure via a cyberattack. Iran has used cyberattacks to conduct retaliatory strikes against the U.S. in the past and possesses a significant offensive cyber capability, including the ability to destroy data, disrupt computer networks and cause significant financial loss. If cyberattacks against other U.S. critical infrastructure or entities occur, collateral damage or disruption to health care operations may result.

For example, in November 2018, Iran-based hackers were indicted by the FBI for developing and deploying the SamSam ransomware, which also targeted U.S. hospitals and health care organizations. In March 2018, nine Iranians were indicted for conducting a massive hacking campaign on behalf of the IRGC, which targeted universities including academic medical centers. In 2016, seven Iranians working on behalf of the IRGC were indicted for conducting denial of service attacks against U.S. financial institutions and accessing the control system of a small dam.

**Hospitals and health systems should assess their cybersecurity posture with special emphasis on:**

- Patching of critical cyber vulnerabilities, especially those present in medical devices or mission critical systems, which could impact care delivery operations and patient safety. Assess backup and manual operation capability of life-saving medical devices.
- Reminding staff to be especially vigilant for possible spear phishing emails and not click on suspicious or unexpected emails and/or attachments.
- Assessing and testing of email security, intrusion detection and response systems.

- Assessing of dependencies and cybersecurity of network connected mission critical systems, such as utilities (especially power supply), HVAC and access control systems. It's also important to assess redundancy and manual override capability of these systems.

- Assessing and testing of backup security, redundancy and restoration times – ensuring backups are offline, with multiple copies on site and cloud-based, on different media types.

- Vendor risk management program – reviewing cybersecurity requirements and dependencies on mission critical vendors and those that have remote or direct access to sensitive data, operations, backups and locations. Identify high-risk vendors – and their subcontractors – especially those based overseas.

- Reviewing, updating and testing a unified, cross function cyber incident response plan, which incorporates a designated cyber response firm and local FBI Cyber Task Force Point of Contact.

- Reviewing sufficiency and limitations of cyber insurance for your organization and your vendors, including any "act of war" exclusions.

- Reviewing additional cyber defensive measures distributed by the FBI on April 9, 2019, in response to increased cyber threats posed by IRGC.

**The AHA will continue to monitor this developing situation in close coordination with government agencies. Please visit AHA's cybersecurity webpage for more resources. For further information on this issue or other cybersecurity topics, please contact AHA Senior Advisor for Cybersecurity and Risk and former FBI Cyber Senior Executive John Riggi at jriggi@aha.org.**

© 2020 American Hospital Association | www.aha.org