Barley Snyder

Feds Warn of Cybersecurity Threats Against Health Care

PUBLISHED ON
November 9, 2020

Health care companies and organizations could soon be the victims of cyberattacks, according to a recent warning from federal authorities.

In a joint statement from three different federal groups, including the FBI, there is "credible information of an increased and imminent cybercrime threat to U.S. hospitals and health care providers."

The statement said the ransomware attacks already hit four hospitals this fall. A cyberattack on September 29 hurt the 250 hospitals of Universal Health Services Inc.

The report specifically pointed to ransomware, a form of malicious software infecting a computer or infrastructure. The ransomware shuts down a computer system and demands money to allow your system to return to normal.

The federal agencies didn't specifically list the methods to avoid this particular ransomware, but instead offered a list of proven ways to keep your system safe from ransomware, including:

- Join in with cybersecurity organizations, such as the Health Information Sharing and Analysis Center
- Follow ransomware best practices
- The Cybersecurity and Infrastructure Security Agency (CISA) has no-cost resources for companies, including health care organizations
- Federal security authorities have resources it could offer a company depending on how much a company is willing to share of its confidential materials and methods

Health care organizations have been stretched thin because of the COVID-19 pandemic. While the initial wave may have subsided, rising case numbers across the country hint at what could be any phase of the pandemic that could further divert a health care organization's attention from their cyber protection.

Cyber criminals have been known to prey on weakened security systems, which could include companies where their attention may be focused elsewhere - as with the health care and hospital system on the frontlines of trying to slow the spread of the COVID-19 pandemic.

Health care organizations should take serious heed to this federal warning. They should work with their own information technology professionals and even consider bringing in outside IT professionals to at least audit their own security systems.

If you have questions on how your health care organization - or any other company - can mitigate the cyber threats against it, contact any member of the Barley Snyder Cybersecurity Service Team.

:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com

Elizabeth L. Melamed

Associate

Tel: 717-399-1538

Email: emelamed@barley.com