KAUFMAN | DOLOWICH

Federal Agencies Warn of an Imminent Ransomware Threat Against U.S. Hospitals

By: Eric Stern, LI Partner and Co-Chair of the Data Privacy and Cybersecurity Practice Group

The FBI, DHS, & HHS has warned of an imminent and credible ransomware threat against U.S. hospitals.

According to an alert today from the Cybersecurity and Infrastructure Security Agency (CISA) "CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers. CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats."

It is recommended that entities in the health care field "maintain business continuity plans—the practice of executing essential functions through emergencies (e.g., cyberattacks)—to minimize service interruptions." CISA, FBI, and HHS suggest HPH Sector organizations review or establish patching plans, security policies, user agreements, and business continuity plans to ensure they address current threats posed by malicious cyber actors.

Furthermore, health service providers should make their employees aware of the threat and remind them to not open emails or click on links unless they are confident in the identity of the sender. As the alert advises, employers should "Focus on awareness and training. Because end users are targeted, make employees and stakeholders aware of the threats" and "ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim of a cyberattack."

We recommend that all companies – whether threat is imminent or not — continuously review and update their security systems and develop response and reporting protocols, as put together with the assistance of counsel.

For more details on the threat, please follow this link: https://us-cert.cisa.gov/ncas/alerts/aa20-302a