White and Williams LLP

Federal Advisory Warns Hospitals Facing "Increased and Imminent" Cyber Threat; 400 Hospitals Already Targeted

By: Debra A. Weinrich, Charles Eppolito, III and Joshua A. Mooney
Cyber Law and Data Protection and Healthcare Alert
10.30.20

A Joint Cybersecurity Advisory (the Advisory) by the Cybersecurity & Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the Department of Health & Human Services (HHS) has warned of an increased and imminent threat against U.S. hospitals. This week, the ransomware Ryuk hit at least six U.S. hospitals in a 24 hour period. *The New York Times* reported that "[h]undreds of American hospitals are being targeted in cyberattacks by the same Russian hackers who American officials and researchers fear could sow mayhem around next week's election." Warning of "an increased and imminent" cyber threat to U.S. hospitals and healthcare providers, the Advisory's key findings are:

- CISA, the FBI and HHS assess malicious cyber actors are targeting the HPH Sector with TrickBot and BazarLoader malware, often leading to ransomware attacks, data theft and the disruption of healthcare services; and
- these issues will be particularly challenging for organizations already dealing with the COVID-19 pandemic; therefore, administrators will need to balance this risk when determining their cybersecurity investments.

Deployment of the malware, the advisory states, largely results from successful phishing campaigns. Many times, these emails "can appear as routine, legitimate business correspondence about customer complaints, hiring decisions, or other important tasks that require the attention of the recipient." Some email communications have included the recipient's name or employer name in the subject line and/or email body.

The Advisory comes on the heels of advisories from the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) in the U.S. Department of the Treasury warning ransomware victims, their insurers and their incident response teams of potential sanctions for facilitating ransomware payments. The OFAC-directed advisory, in particular, warned that "engaging in transactions, directly or indirectly, with individuals or entities ('persons')" designated by OFAC as threats to national security, some of whom like Evil Corp and the Lazarus Group are well known for their ransomware exploits, can result in federal prosecution and significant sanctions.

The Advisory provides recommendations and best practices that hospitals and other healthcare providers should incorporate immediately. They include the aforementioned business continuity plans for executing essential functions through service interruptions caused by cyberattacks and other emergencies (*e.g.*, cyberattacks); network best practices, such as updated patching processes, security policies and user agreements to address current threats posed by malicious cyber actors; and ransomware best practices like:

- regularly backing up data, air gapping and password protect backup copies offline; and
- implementation of a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, secure location.

The Advisory also cautions against paying ransoms.

Prevention and mitigation are key. Much of the mitigation available requires working closely with cyber counsel and IT specialists, but it does not end there. Business continuity plans are encouraged as hospitals and healthcare providers need to ensure they are ready to safely perform essential functions if their computer systems are attacked.

Additionally, while the agencies correctly encouraged review and implementation of business continuity plans and procedures, and even provided some details about the associated risks and mitigation, there are important aspects of policies, procedures and plans which are even broader. For instance, the following issues or questions should be considered as they may have a direct impact on clinical care and the possibility of medical malpractice suits:

- How is your clinical practice or institution going to process lab orders and ensure results are available and distributed?
- How will you handle dictation and/or entries into the electronic medical record to ensure that necessary and appropriate clinical documentation is created and saved?
- Have you instituted appropriate policies, protocols and training of your staff designed to ensure continuity of care in the event of cyberattack emergency?

It is essential that healthcare providers proactively consider and address the impact a cyberattack could have on clinical services, including review and revision of business continuity plans. Advice from your legal cyber counsel can help.

If you have questions or would like further information, please contact Debra A. Weinrich (weinrichd@whiteandwilliams.com; 215.864.6260) or Charles Eppolito (eppolitoc@whiteandwilliams.com; 215.864.6302).