COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 1. January 13, 2022 2022 Outlook: More Dangerous Ransomware Coupled With Inadequate Security Practices

By Jane Anderson

As the COVID-19 pandemic enters its third year, real "security fatigue" with pandemic-related issues will combine with cybercriminals' increasingly sophisticated capabilities to create an acceleration of ransomware and other security incidents, cybersecurity experts predict.

The threats of this year will look like those seen in 2021, with the caveat that they're likely to be worse, three experts told *RPP*. They warned covered entities (CEs) and business associates (BAs) to be wary of unsecured Internet of Things (IoT) devices, cobbled-together systems that allow staff to work on-site or at home, and lapses in performance of basic security strategies.

"Going into 2022, we will see more cyber threats directed against hospitals, especially ransomware attacks," said Chuck Everette, director of cybersecurity advocacy at cybersecurity company Deep Instinct. "In 2020 and 2021, ransomware criminal gangs have found that targeting and attacking hospitals, outpatient clinics and other health care facilities during the time of a global pandemic is lucrative."

In fact, HHS Secretary Xavier Becerra used his first-ever end-of-year message to warn of the "urgent need to remain vigilant against cybersecurity threats," and noted that cybersecurity experts have identified a vulnerability in Apache Log4j, a "ubiquitous piece of software that exists in thousands of applications—including control systems for medical devices and hardware—that, if exploited, could result in data exfiltration or ransomware and significantly disrupt your ability to deliver health care and pose a threat to national security."[1]

Becerra recommended that health care organizations:

- Implement the guidance issued by the Department of Homeland Security Cybersecurity & Infrastructure Security Agency (CISA) for the Apache Log4j information.[2]
- Review cybersecurity resources from HHS and CISA.
- Diligently monitor networks, raise cybersecurity awareness, and maintain readiness of emergency operations procedures and continuity plans.
- Promptly report any cybersecurity incidents to CISA or the FBI.

"As health care and public health leaders, we rely on your vigilance and partnership to protect our country from nefarious actors looking to disrupt or exploit our critical health infrastructure," Becerra wrote.

The COVID-19 pandemic has allowed cybercriminal gangs to expand and grow their own networks by leveraging many businesses' hybrid work-from-home model, plus migrations to the cloud, Everette said. "This has greatly expanded the health care industry footprint, in turn increasing the attack surface for these cybercriminals, creating a target-rich environment. Add in the sense of urgency to recover quickly from a cyberattack, and health care organizations typically will pay ransoms quickly in order to get back online and limit client impact. This also

has resulted in cybercriminals increasingly attacking health care more [often], due to the rapid ransom payday."