COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 1. January 31, 2019 Look for Complex, Believable Spear Phishing Attacks, More Dangerous Ransomware in 2019

By Jane Anderson

Phishing attacks will continue to become more sophisticated as 2019 gets underway. That means health care IT professionals will need to ramp up their game with increased training and augmented incident response plans, health cyber experts say.

Attacks using the internet of things (IoT) and malware embedded in devices also are expected to increase, experts tell *RPP*, so covered entities (CEs) and business associates (BAs) should anticipate those threats as well. Roger Shindell, president and CEO of Carosh Compliance Solutions, believes that cyberattacks, including phishing and ransomware, will be more advanced than they were even a year ago, and will involve more complex technology, including some sponsored by foreign states.

"The health care industry will continue to be the top target of cyberattacks," adds Michelle O'Neill, director of corporate compliance, Summit Health Management in New Jersey. "The cyberthreat environment is becoming more and more dangerous. Although many of the threats may be consistent [with] what we have seen in 2018, the major difference is that these attacks will be sophisticated."

Rebecca Herold, president of SIMBUS360.com and CEO of The Privacy Professor, says she sees targeted ransomware attacks as a top cyberthreat in 2019. "Ransomware has been making the crooks…millions of dollars year after year," she says. "The majority of health care organizations are paying the ransoms, so of course the crooks see this as a cash cow revenue path. They will increase their efforts, expand their methods and increase their ransom demands in 2019."

At least three of the top six protected health information (PHI) breaches reported in 2018 involved either phishing or ransomware:

- UnityPoint Health in Des Moines, Iowa, began notifying 1.4 million patients in July that a phishing attack had compromised its business email system and may have resulted in unauthorized access to PHI. The phishing emails appeared to come from a trusted executive within the company, UnityPoint Health said in its statement.
- In a breach that involved more than 502,400 people, Health Management Concepts (also known as HMC Healthworks), based in Jupiter, Florida, paid the ransom to release its data following a ransomware attack in July but, in the process, accidentally provided the attackers with a file containing PHI.
- Augusta University Health in Georgia reported breaches involving about 417,000 people that resulted from phishing attacks. Those breaches occurred in September 2017, but the university said it didn't learn that data had been breached until July 2018.

The top attack vector involving health care will continue to be phishing, just as it was in 2018, O'Neill says. However, phishing attacks will be more targeted this year, she says, and mobile phishing is on the rise due to the increasing amount of data that is collected from sites and apps visited on mobile devices. "This leaves individuals

open to a very pointed and targeted phishing attack," she says.