COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 4. April 30, 2018 Prepare for Ransomware Attack With Archived Forms, Offline Records, and Constant Practice

By HCCA Staff

Hackers hit the 911 emergency system of Baltimore, Maryland; the city of Atlanta, Georgia; and Boeing Co. with ransomware demands late last month. Experts warn that health care entities need to rehearse their responses to potential ransomware attacks, and keep offline backups of everything.

“If you want to prepare to deal with a ransomware attack, our organizations need to practice disaster recovery and business continuity,” says Joseph Kirkpatrick, managing partner for KirkpatrickPrice in Tampa, Florida. “The more you practice, the better you’ll get at it and the faster you’ll be able to recover. How do you go from having all your systems down to getting back up again? You’re talking about an IT staff that will be taxed. This is why you need to practice the whole thing.”

International rings of opportunists are deploying increasingly sophisticated ransomware attacks, and government services, schools and hospitals have been particularly hard hit so far in 2018.

For example, in Atlanta, the hackers released the malware SamSam, which also was blamed for a major ransomware attack on Erie County Medical Center (ECMC). SamSam is estimated to have facilitated the extortion of more than $1 million from 30 organizations this year and is known to be used against targets most likely to pay the ransom. Hospitals are high on the list of targets, Kirkpatrick says.

Atlanta’s ransomware attack began on March 22 and shut down applications city residents use to pay bills and access court-related information. Ten days later, the Municipal Court of Atlanta was rescheduling hearings, and city residents couldn’t pay traffic tickets and water bills. No health-related apps were reportedly involved. Baltimore’s ransomware attack, meanwhile, shut down its 911 dispatch system for 17 hours beginning March 25. Some Boeing computers were hit by the WannaCry malware on March 28.

Other ransomware incidents affecting health care entities have included last year’s more widespread WannaCry attacks and Petya/NotPetya attacks. The WannaCry incidents mostly passed over U.S.-based health care entities but hit the U.K.’s National Health Service hard, knocking many NHS offices offline for several days or more (*RPP 6/17, p. 1*). The Petya attacks caused damage that required at least one hospital to replace parts of its computer systems.