"A Cybersecurity Update and Resource Guide for Healthcare Organizations"

Richard S. Cooper, James J. Giszczak, Rick L. Hindmand | Tuesday, July 18, 2017

In the wake of the recent WannaCry Ransomware cyber attack that is believed to have started at Britain's National Health Services (NHS) before quickly spreading to more than 200 countries, the U.S. government is urging the healthcare industry to take further precautions regarding cybersecurity and is deploying tools to assist organizations in responding to immediate threats and implement stronger security measures.

WannaCry Ransomware

On May 12, 2017, the WannaCry Ransomware worm infected the information systems of 47 NHS organizations and caused widespread disruption of patient care and operations at NHS hospitals and facilities, including the interruption of telephone communications and the instantaneous loss of access to patient records, etc. As WannaCry continued to spread rapidly across the globe, NHS, the U.S. government and experts from the private sector collaborated to warn the public at large and attempt to develop a patch.

The WannaCry attack and the rise of sophisticated ransomware attacks paralyzing operations and patient-critical devices underscore the vulnerability of the healthcare system in the U.S. and abroad. Today, digital connectivity in the healthcare industry is ubiquitous and paramount to the safe and efficient delivery of patient care. But the risks are real and multi-faceted—fraud, identity theft, data privacy breaches, ransomware, supply chain disruptions, research and development theft, stock manipulations, etc. Such

risks add exponentially to the already complex (and at times conflicting) state, federal, and payordriven framework of rules and regulations inherent to the U.S. healthcare industry.

Click here to read the entire article in the AMCNO Northern Ohio Physician.

Richard S. Cooper

Team member bio

James J. Giszczak

Team member bio

Rick L. Hindmand

Team member bio