A PUBLICATION OF LAW BULLETIN MEDIA

CHICAGO LAWYER®

OCTOBER 2018

MED-MAL MATTERS

MEET 'PESTILENCE'

Medical-record hacking can kill

By THOMAS A. DEMETRIO and KENNETH T. LUMB

Recent high-profile data breaches involving retailers, a credit reporting agency and various governmental entities have illustrated the vulnerability of electronically stored, private information. Patient health data is arguably among the most personal and sensitive of this private information and according to cybersecurity experts, it is a high-value target for blackmail, ransom and identity theft. A new study has revealed, however, that improperly secured medical record systems and medical devices are jeopardizing not only patient privacy, but also patient safety.

At the 2018 Black Hat conference in Las Vegas, described by organizers as "the world's leading information security event," researchers from University of California, San Diego, and University of California, Davis, showed that hackers can easily modify medical test results remotely by attacking the interface between hospital laboratory devices and medical record systems.

Researchers did not actually hack an existing electronic record system. Instead, according to UC, San Diego, they built a virtual system consisting of medical laboratory testing devices, computers and servers. They then used what is known as a "man in the middle" attack, in which a computer inserts itself between the laboratory device and the medical records system. The team, which consisted of physicians and a computer science graduate student, was then able to run tests, intercept the test results, modify or manipulate those results and then send them to the electronic records system.

In one iteration, researchers modified normal blood test results to make it appear as if the patient was suffering from diabetic ketoacidosis, an excess of ketones in the blood related to high blood glucose. Insulin, the treatment for DKA, could in turn be deadly for a patient with normal or low blood glucose. The researchers also changed normal blood tests to indicate a low potassium level, which would generally lead to administration of potassium through IV fluids. That treatment in a patient with a normal potassium level, however, could cause a fatal heart attack.

The methods used, which the researchers aptly named Pestilence, exploit vulnerabilities arising from the standards used to transmit data within hospital networks. These standards, known as the HL7 standards, are published by Health Level Seven International, a not-for-profit, American National Standards Institute-accredited standards developing organization.

The HL7 standards, which are used to design the code that allows all devices and systems in a facility to communicate, were developed in the 1970s but have "remained untouched by many of the cybersecurity advances made in the last four decades," according to UC, San Diego.

To make matters worse, for years, personnel with little or no cybersecurity training have implemented the standards on "aging" medical equipment in an unsecure fashion, transmitting plain text on networks that lack passwords or any other forms of authentication.

While many data breaches can lead to financial loss and untold frustration, the vulnerabilities laid bare by Pestilence endanger human life itself. To protect patients, health-care institutions must improve their network security practices, the Pestilence researchers advise.

For instance, all medical record systems and medical devices should be password-protected and secured behind a firewall. Hospitals also need to ensure that each device and system on the network can only communicate with one server, a method known as network segmenting that limits a hacker's ability to infiltrate an entire system.

In addition to hardware and software vulnerabilities, the Pestilence researchers identified a familiar hospital-related deficiency: Lack of training. More than 80 percent of hospital IT personnel have no training in cybersecurity.

Finally, the researchers make a very convincing argument for action by the FDA. The cybersecurity deficiencies of medical devices and systems will never be properly addressed unless the FDA's approval process includes a very hard look at cybersecurity and manufacturers are required to adopt the latest and most secure operating systems.

For example, many medical devices in operation still run on Windows XP, an operating system released in 2001 that is no longer supported by Microsoft, which means that bugs and vulnerabilities are not fixed — a continuous process necessary for any operating system used in even the most basic home computer.

Kind of like equipping an intensive care unit with iron lungs instead of mechanical ventilators. American health-care consumers deserve better. CL

Thomas A. Demetrio is a founding partner of Corboy & Demetrio, representing victims of medical malpractice and personal injury.
TAD@CorboyDemetrio.com

Kenneth T. Lumb is a medical-malpractice attorney and partner at Corboy & Demetrio.
KTL@CorboyDemetrio.com