Clear tactics, but few easy solutions, for hospitals combating ransomware

September 19 2017, by David Orenstein

Hospitals face a serious crisis when hackers seize control of computers, effectively locking down patient records, in "ransomware" attacks. Credit: Brown University

Especially cruel hackers know that lives are on the line when they hold a

hospital's computer systems hostage, as they did in the May 12 attack dubbed WannaCry, which locked down many overseas hospitals with the demand for a ransom. In a new article in the *Annals of Internal Medicine*, three medical and legal experts delineate the many steps hospitals can take to prevent and respond to attacks, but note that some strategies won't be easy to accomplish and that full security is likely impossible to ensure.

"Patients can suffer severe negative health effects if their treatment is delayed, discontinued or performed incorrectly because hospital records are unavailable," the authors wrote in the essay titled "Your Money or Your Patient's Life: Ransomware and Electronic Health Records."

The authors are Dr. Eli Adashi, professor of medical science and former dean of medicine and biological sciences at Brown University; I. Glenn Cohen, professor of law at Harvard University; and Sharona Hoffman, professor of law and bioethics at Case Western Reserve University.

"There are things we can do to reduce the risk but it is very hard to perfect IT security, especially given the needs of modern hospital systems to have things moving between places and increasing demand for patient-facing access," Cohen said. "To some extent, these attacks are inevitable."

The authors cite research that counted nearly 2,000 hospital data breaches of varying kinds between 2009 and 2016. In that last year, a ransomware attack hit a hospital system in the Baltimore area, forcing workers to rely on paper records.

In their new paper, the authors list several steps—some simple and others more complex—that hospitals can take to prevent or at least mitigate attacks and to ensure that they are in compliance with the Health Insurance Portability and Accountability Act, which requires

holders of health records to keep them secure. Some of the more straightforward tactical recommendations include workforce training, retaining cybersecurity expertise, patching operating systems and reporting attacks promptly to authorities.

But they also recommend more strategic, nationwide steps, even though those may be harder to accomplish.

Adashi noted that the U.S. government's response in the wake of WannaCry was fragmented among many agencies, although just the day before President Donald Trump had issued a sweeping executive order instructing federal agencies to embark on a number of actions to ensure greater cybersecurity. Building on that to develop a cohesive government response pertaining to health care infrastructure, he said, could provide all hospitals with common, well-informed guidelines.

"We need a coordinated national effort," he said. "This will take time."

Cohen said another key step could be for the Joint Commission, which accredits hospitals, to make cybersecurity requirements a high priority in renewing accreditation.

And hospitals should consider committing to a principle of "non-payment" of ransoms to hackers, the authors proposed, akin to the US government policy of not paying ransoms to terrorists. Adashi said all of these steps, but especially that one, should be implemented only after considerable public discussion.

After all, with lives on the line, Cohen acknowledged, pressure could quickly build to abandon an abstract policy, especially if it didn't have buy-in from patients.

"If I were a hospital CEO, it's one thing to make this pledge ex ante, but

it's another thing when you have a population of patients who need health care to stick by it," he said.

More information: *Annals of Internal Medicine*, DOI: 10.7326/M17-1312 , annals.org/aim/article/2654048 … ronic-health-records

Provided by Brown University