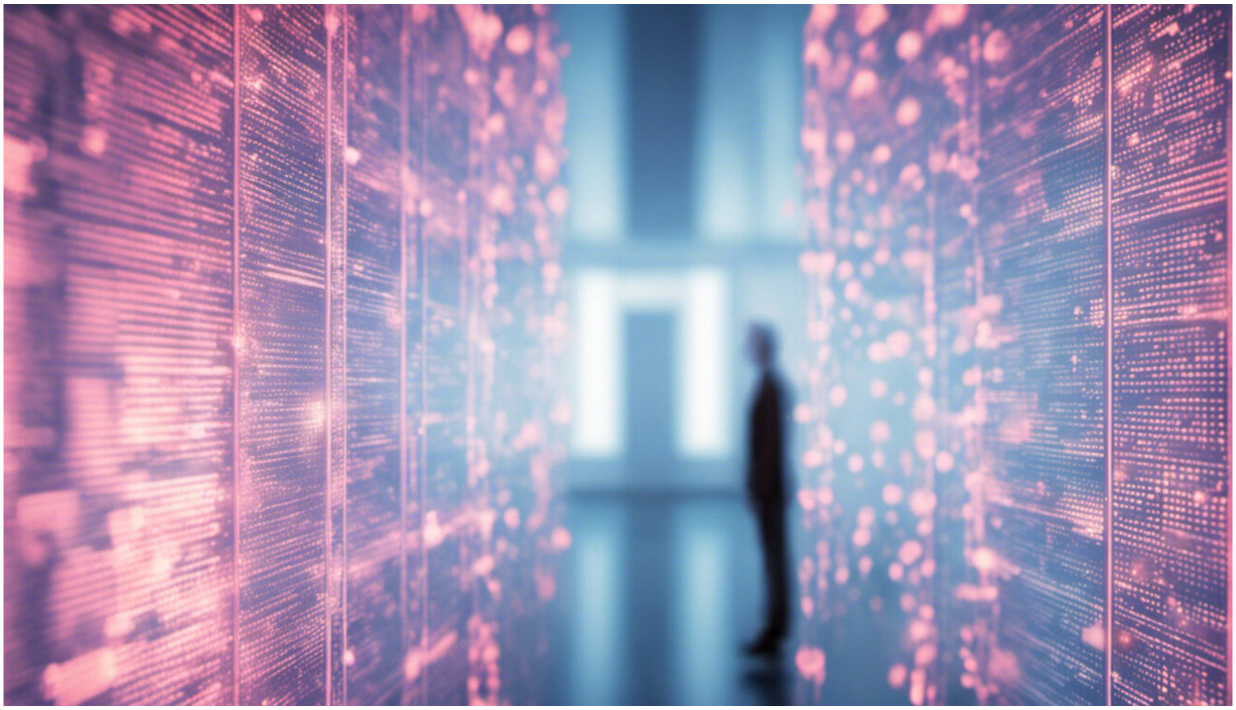
PHYS.ORG

Defending hospitals against life-threatening cyberattacks

April 25 2018, by Mohammad S. Jalali



Credit: AI-generated image (disclaimer)

Like any large company, a modern hospital has hundreds – even thousands – of workers using countless computers, smartphones and other electronic devices that are vulnerable to security breaches, data thefts and ransomware attacks. But hospitals are unlike other companies in two important ways. They keep medical records, which are among the most sensitive data about people. And many hospital electronics help keep patients alive, monitoring vital signs, administering medications, and even breathing and pumping blood for those in the most dire conditions.

A 2013 data breach at the University of Washington Medicine medical group compromised about 90,000 patients' records and resulted in a US$750,000 fine from federal regulators. In 2015, the UCLA Health system, which includes a number of hospitals, revealed that attackers accessed a part of its network that handled information for 4.5 million patients. Cyberattacks can interrupt medical devices, close emergency rooms and cancel surgeries. The WannaCry attack, for instance, disrupted a third of the UK's National Health Service organizations, resulting in canceled appointments and operations. These sorts of problems are a growing threat in the health care industry.

Protecting hospitals' computer networks is crucial to preserving patient privacy – and even life itself. Yet recent research shows that the health care industry lags behind other industries in securing its data.

I'm a systems scientist at MIT Sloan School of Management, interested in understanding complex socio-technical systems such as cybersecurity in health care. A former student, Jessica Kaiser, and I interviewed hospital officials in charge of cybersecurity and industry experts, to identify how hospitals manage cybersecurity issues. We found that despite widespread concern about lack of funding for cybersecurity, two surprising factors more directly determine whether a hospital is well protected against a cyberattack: the number and varied range of electronic devices in use and how employees' roles line up with cybersecurity efforts.

A wide range of devices

A major challenge in hospitals' cybersecurity is the enormous number of devices with access to a facility's network. As with many businesses, these include mobile phones, tablets, desktop computers and servers. But they also have large numbers of patients and visitors who come with their own devices, too – including networked medical devices to monitor their health and communicate with medical staff. Each of these items is a potential on-ramp for injecting malware into the hospital network.

Hospital officials could use software to ensure only authorized devices can connect. But even then, their systems would remain vulnerable to software updates and new devices. Another key weakness comes from medical equipment offered as free samples by device manufacturers who operate in a competitive market. They're often not tested for proper security before being connected to the hospital network. One of our interviewees mentioned: "In hospitals … there's a whole underground procurement process whereby medical device vendors approach clinicians and give them lots of stuff for free that eventually makes its way on to our floors, and then a year later we get a bill for it."

When new technologies bypass regular processes for purchase and risk assessment, they aren't checked for vulnerabilities, so they introduce even more opportunities for attack. Of course, hospital administrators should balance these concerns against the improvements in patient care that new systems can bring. Our research suggests that hospitals need stronger processes and procedures for managing all these devices.

Staff buy-in

Getting hospital administrators to understand the importance of cybersecurity is fairly straightforward: They told us they're worried about costs, institutional reputation and regulatory penalties. Getting medical staff on board can be much more difficult: They said they're focused on patient care and don't have time to worry about cybersecurity.

People typically treat cybersecurity protections as secondary to what they're trying to get done. One person we interviewed described why some staff committed the cardinal cybersecurity sin of sharing a password: "To use an ultrasound machine [you need a password, which] has to change every 90 days. [Staff] just want to use the ultrasound machine. It's not holding a lot of patient data … so they create a shared login so that they can provide patient care."

The needs can vary widely across a hospital, in ways that can be surprising – such as access to sites likely to carry malicious software. A chief information officer at a research hospital told us, "I personally believe that hardcore pornography has no purpose on hospital supported devices. What did I do five years ago? I put up internet content filters that prevented people from navigating to pornography. Within five minutes, the director of psychiatry calls to tell me that we have a grant to study pornography in a medical context [so we had to modify our filters]."

These experiences are why we concluded that budget limitations are not as crucial to hospital cybersecurity as employee involvement. A hospital can buy as many pieces of hardware and software as it wants. If workers aren't following organizational procedures, the technology won't keep hospitals safe. Our research suggests that cybersecurity is as much about managing people as it is about technology.

Compliance is not security

The threat is nationwide, and keeps getting harder to defend against, as one chief information security officer told us: "The nature of attacks is increasingly sophisticated. It used to be my biggest threat was … students. Today, it's state-sponsored attacks, terrorism and organized crime. It's more threats than ever before of a more serious nature."

Unfortunately, many hospital administrators seem to believe that protecting data is as simple as meeting state and federal regulations. But those are minimum standards that don't adequately address the threat. As one of our interviewees said, "Compliance is a low bar. I guarantee that little health care organizations and hospitals would do nothing (without regulation). They would have a piece of paper on a shelf called their security policy. It's needed as a backstop to get companies at least thinking about it. But being compliant does not solve the greater risk management problem."

Our research shows that hospitals need to think beyond compliance. Also, with so few hospitals well defended against cyberattacks, all hospitals appear more attractive as potential targets. In our view, it's not enough for hospitals to improve their own defenses – nor for regulators to raise standards. They should manage, and evaluate the security of, the devices on their networks and ensure medical staff understand how good cyber-hygiene can support good patient care. Further, policymakers, health care leaders and hospitals themselves should work together to make the industry as a whole less susceptible to attacks that threaten people's privacy and their very lives.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Defending hospitals against life-threatening cyberattacks (2018, April 25) retrieved 23 April 2024 from https://phys.org/news/2018-04-defending-hospitals-life-threatening-cyberattacks.html