

Health care's huge cybersecurity problem

The patient lying on the emergency room table in front of Paul Pugsley was having a stroke. Time was running out. Pugsley, an emergency medicine resident at Maricopa Medical Center, knew he needed to send the patient for a CT scan.

But when Pugsley looked over at the computer screen at the side of the room, he saw a pop-up message demanding bitcoin payment. A few minutes later, he was told that the same message had shut down the scanner – he'd have to help the patient without knowing whether the stroke was caused by a bleed or a clot, information that's usually vital to the course of treatment.

After a few minutes of frantic workarounds, the patient – actually a medical test dummy – was wheeled out the room (prognosis: survival, but serious brain damage). The flashing ransom note was part of a simulation, designed to expose physicians like Pugsley to the very real threat of cyberattacks on their hospitals.

Reports show that ransomware and other cyberattacks are on the rise – and health care is one of the biggest targets. Just this week, researchers in Israel announced that they'd created a computer virus capable of adding tumors into CT and MRI scans – malware designed to fool doctors into misdiagnosing high-profile patients, Kim Zetter reports for *The Washington Post*. Despite the rising threat, the vast majority of hospitals and physicians are unprepared to handle cybersecurity threats, even though they pose a major public health problem.

The health care industry increasingly relies on technology that's connected to the internet: from patient records and lab

results to radiology equipment and hospital elevators. That's good for patient care, because it facilitates data integration, patient engagement, and clinical support. On the other hand, those technologies are often vulnerable to cyberattacks, which can siphon off patient data, hijack drug infusion devices to mine cryptocurrency, or shut down an entire hospital until a ransom is paid.

"If systems are disrupted over the internet, by an adversary or an accident, that can have a profound impact on patient care," says Beau Woods, a cybersecurity advocate and cyber safety innovation fellow with the Atlantic Council.

A screenshot of the WannaCry ransomware.

Image: SecureList / AO Kaspersky Lab

The case Pugsley faced in the simulation mimicked the spring 2017 WannaCry cyberattack, which infected thousands of computers and crippled the United Kingdom's National Health Service. In 2017, the Health Care Industry Cybersecurity Task Force convened by the US Department of Health and Human Services concluded that health care cybersecurity was in "critical condition." Experts say that health care lags far behind other industries, like the financial sector, in the way it protects its information technology infrastructure. And unlike finance, a health care failure can end with injury or even death.

There's no evidence that any patients died as a direct result of WannaCry. But the attack crippled thousands of hospital computers and pieces of diagnostic equipment – forcing doctors to ferry lab results across hospitals by hand and cancel nearly 20,000 patient appointments. The attack targeted vulnerabilities in the Microsoft Windows operating system, encrypting data and holding computer systems for bitcoin ransom. While WannaCry was eventually stymied, Woods says

health care institutions continue to be vulnerable to attacks of that magnitude.

"We know there's kindling on the ground, we just don't know what match is going to light it."

"I want to raise the alarm without being alarmist," Woods says. "The preconditions for something bad to happen are there. We know there's kindling on the ground, we just don't know what match is going to light it."

Billions of threats

NotPetya was one of the largest cyberattacks of all time. The June 2017 attack caused \$10 billion in damage to companies and crippled computers around the world, from Tasmania to Copenhagen – including those at the Massachusetts-based medical transcription service Nuance. The company's systems were shut down for weeks, which left thousands of health care delivery organizations, including Sutter Health, a Northern California health care system, unable to use its programs.

Sutter Health, which serves over 3 million patients, was prepared. They were able to quickly respond to the attack and move off of the system, says chief privacy and information security officer Jacki Monson. But within a day, it still had a backlog of over 1 million files that needed to be transcribed.

"It could have easily created a patient safety issue – if you have transplant patients, or patients who are having surgery, you need all those medical notes," she says.

it was hit with around 87 billion cyber threats in 2018

Sutter Health deals with countless cyberattacks daily. It was hit with around 87 billion cyber threats in 2018, according to Monson, and uses artificial intelligence technology to sort and evaluate them. "We prioritize them – a human couldn't look at that many billions." Based on the nature of the threat, the

team might apply software patches, or block an email address that they expect a phishing attack to come from.

The number of threats Sutter Health faces is likely on the high end, due to the size of the system, Monson says – but the number would still be in the billions for any hospital or health care delivery organization. And it only takes one threat to break through. “Most organizations with an active cyberattack in their system don’t discover it for 18 months or longer,” Monson says. “It’s not a measure of when or if – it’s probably already happening and you just don’t know it.”

“Most organizations with an active cyberattack in their system don’t discover it for 18 months or longer.”

Sutter Health’s robust cybersecurity program, though, is an exception rather than the rule. Most hospitals don’t have the resources to monitor threats to their systems, and many might not even be aware that they’re something to be concerned about.

Medical device manufacturers and the Food and Drug Administration are well aware of the challenges around health care cybersecurity: the FDA has guidelines around how medical device makers should manage security risks both before and after products are put on the market, and hosted a workshop on device cybersecurity at the end of January. At the workshop, a group of device makers (including big names like Abbott and Medtronic) committed to working closely with hackers and security researchers on vulnerabilities.

But hospitals and physicians haven’t kept pace with that progress. “We have good tools in the middle of the supply chain, at the FDA level, with manufacturers,” Woods says. “We don’t see it at the actual point of delivering care.”

The costs of black boxes

The technologies inside of hospitals vary widely: some medical

devices are new, but others are made by companies no longer in business, or run on old software with gaping security holes. Pacemakers and other implanted, internet-connected devices are hackable. Human error opens holes in systems, as well: on the data privacy side, most breaches were triggered by employee mistakes or unauthorized disclosures, according to research published in *JAMA Internal Medicine*.

What's more, experts say that hospitals often don't know what systems run on the devices that they use every day. "When WannaCry hit, hospitals were scrambling to figure out which medical devices were impacted," says Christian Dameff, cybersecurity researcher and informatics fellow at the University of California San Diego Health. "These devices are often black boxes to hospitals."

That's not to say that hospitals aren't paying *any* attention to their computing systems. It's just that their focus tends to be on a different kind of security. Data security practices in place in hospitals usually prioritize protecting patient privacy, because organizations can be fined under HIPPA for exposing patient data. "It allows them to gloss over [the fact] that devices that may not have patient health info are subject to the same risks," says Jeff Tully, a cybersecurity researcher and physician at the University of California, Davis Medical Center.

Compounding the issue, the vast majority of hospitals don't have full-time cybersecurity employees, Dameff says. "There's a lack of awareness, and there's a lack of resources," he says. Small, rural hospitals in underserved communities, he notes, probably don't have the money to hire staff or update their systems. And without security staff, they might not be aware of or able to implement security updates announced by a device company.

"There's a lack of awareness, and there's a lack of resources."

Without a protective bulwark, it can be tricky for the people already on staff to even notice that they're under attack. Nurses and doctors, who already have a lot on their plates, might not recognize a hacked device. If, say, an infusion pump delivering a drug was infected with cryptocurrency-harvesting malware, which slowed medication delivery, that device might just be yanked out of a patient room and replaced with the same model, Dameff says, a solution that wouldn't address the underlying problem and could affect patient care.

"One of the scariest things would be a medical device with a vulnerability, but the device is unpatchable," Dameff says. "What can we do? What do we tell patients?" A hospital isn't forced by any regulatory body to update their equipment – and it might not be feasible for them to do so. If a piece of equipment costs \$4 million and can't be fixed, the hospital might not be able to afford to replace it with something new, he says. "They might say, 'We don't have a choice.'"

Caring for patient care

In November, the computer systems at the East Ohio Regional Hospital and Ohio Valley Medical Center suddenly stopped working. They'd been hit by a ransomware attack – forcing the hospitals to divert patients from the emergency room and return to a paper charting system. Staff had trouble accessing bedside ultrasounds and had limited access to CT scans, says Neal Aulick, medical director for emergency services at the hospitals. It was a difficult time, but Aulick notes that "looking back to when we were down, we didn't see bad outcomes, I think we handled it very well," he says.

There's a tension between cybersecurity experts who want to secure hospital systems and doctors who are focused on patient care. It's key for clinicians to understand the importance of cybersecurity, because they're in direct contact with the patients using and affected by medical devices, but it can be

a hard sell for busy clinicians. And without hospital and physician engagement, Dameff says, all the efforts that the FDA and medical device companies put into improving cybersecurity fall short. It's what he calls the last mile problem: "It's that last step where a provider or hospital would have to find a problem, or deploy a [software] patch. That's really hard," he says. "We'll have all this great work like we're supposed to, but then a doctor doesn't install the update."

As an emergency medicine physician and medical director, Aulick says that he recognizes the risks of internet-connected systems, but says that has to be balanced against the benefits of the speed and information for which they allow. "When you have a breach like this, the response is exaggerated," he says. Cybersecurity teams will beef up security with additional passwords or authentication, which makes systems safer, but might also slow down treatment.

"Security adds inconvenience by design. The next step is figuring out how to improve it without the inconvenience."

Sung Choi, assistant professor at the University of Central Florida department of health management and informatics, says that's a common physician response. "Hospitals try to improve security, but in practice, these measures can get bypassed by clinicians, and then they're not as effective," he says. "Security adds inconvenience by design. The next step is figuring out how to improve it without the inconvenience."

And it really can be inconvenient. Even attacks on patient privacy, which might seem separate from patient care, can affect health: Choi's research shows that data breaches increase a hospital's 30-day mortality rate. That might be because the efforts organizations make to recover after a data breach can affect normal operations and pull resources away from patient care. "It introduces a lot of changes to a hospital," he says. "They might need to upgrade software, or retrain staff, and that might affect the clinical workflow."

That's exactly what worries physicians like Aulick. And one of the most difficult tasks that cybersecurity experts face is communicating the importance of a growing and relatively new problem. The fact is, there just isn't a lot of research that has looked into patient health during and after cybersecurity attacks on hospitals.

But there are some analogies. In 2017, research published in the *New England Journal of Medicine* found that people who had heart attacks and were taken to the hospital when a marathon was going on were more likely to die within the month than people taken to the hospital on another day: likely because road closures and a diversion of resources created delays in patient care. It's an imperfect comparison, Tully says, but it's what concerns cybersecurity experts when they think about ransomware attacks. "Anything that results in the delay or degradation of care will affect outcomes," he says.

Framing cyberattacks as safety issues helps experts get physicians and clinicians on board with good cybersecurity practices, when they might otherwise think of it as just an administrative concern, Monson says. "Telling more stories about the impact on the safety of patients resonates with physicians," she says. "If we're not talking about it as patient safety, it's a lower likelihood physicians will understand how it implicates them."

"We don't want to turn clinicians into hackers"

Substantially addressing cybersecurity in health care situations isn't going to be easy, and will take cooperation from everyone from doctors to nurses, to IT professionals and manufacturers. In practice, that might look like adding cybersecurity training to medical schools, or ramping up the use of simulations that place clinicians like Pugsley in situations mimicking a cyberattack. "We don't want to turn clinicians into hackers," Dameff says, "but is it reasonable to have an hour or two or more of cybersecurity training and patient safety as a part of medical school?"

Education on the physician end is important, and Monson notes incentives for hospitals to invest are going to be key, as well. "And at some point, we're going to need regulatory intervention to push the dial," Monson says. "It doesn't seem like voluntary is working. For patient safety, we shouldn't be taking the chance."

Right now, if something like WannaCry hit the United States, Woods says that our hospital infrastructure would be unprepared. "We'd have to make up a response on the fly." The ongoing work to try to bring health care up to speed on best practices is exciting, and there's demand for information from patients and investors. But lives are still at risk, he says. "There's a lot going on. My fear is that it won't be fast enough."

<https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation>