COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 3. March 10, 2022 Securing Problematic 'Legacy' Devices: Be Part of Procurement, Push for Info

By Theresa Defino

Typically a "legacy" describes the lasting impact of an influential person or movement, most often in a positive sense. Not so with medical devices. When legacy is applied to a CT scanner, infusion pump or even the information technology (IT) that runs them, it typically means bad news.

Legacy devices are one of the "key challenges" facing every health care organization, said Kevin Fu, and what to do about them "is the elephant in the room." Such devices will always exist, he said, and "the challenge is going to be, how do we manage that legacy [device] in a very controlled manner?"

It turns out that Fu—and emergency room physician Dr. Christian Dameff—actually have quite a few recommendations for what to do about these devices. In addition to suggestions that involve government action, they offer strategies that health care organizations can implement to prevent cybersecurity incidents and breaches involving what are often life-saving machines.

In February 2021, Fu, an associate professor of electrical engineering and computer science at the University of Michigan, began a one-year position as the inaugural acting director of medical device cybersecurity at the Food and Drug Administration (FDA) Center for Devices and Radiological Health. Dameff is medical director of cybersecurity for UC San Diego Health and assistant professor of emergency medicine, biomedical informatics, and computer science at the University of California San Diego.

Dameff recently described the need for health care organizations to develop department-specific cybersecurity incident response or disaster plans to address vulnerable devices.[1]

In addition to emerging cyber threats, health care organizations universally are struggling with legacy devices, which are not only "known to be insecure but are actually insecurable," Fu said, which can happen when a manufacturer no longer supports the device via software patches and updates.

Fu joined Dameff during a webinar sponsored by ECRI,[2] a follow-up to its 15th annual Top Ten Health Technology Hazards for 2022.

Yet, it should not come as a surprise to officials that a medical device is using an old Windows program, Fu said. "Anybody should be able to figure out what operating system comes on a medical device and should have some kind of plan, because Microsoft publishes the day that they end support of those operating systems," he said.

Beware Obligations Under HIPAA

Fu added that health care organizations, under the security rule, not only have to safeguard protected health information but assure both the availability and the integrity of it to deliver patient care. Some ransomware itself and the remediation process afterward have led to facilities being unable to access patient records and, in some cases, deliver radiation therapy to cancer patients, Fu said.

"We have not yet picked up on signals of ransomware causing harm to integrity, but I know, as an engineer, that is very possible," said Fu. He added that "some really strange integrity problems can happen on a medical device…and we might actually in the clinical setting unknowingly be using a device that's been effectively adulterated by ransomware or other kinds of malware, without realizing it."

He called problems with the integrity of devices "a red flag and a bit of a signal saying there are problems to come."

Device manufacturers need to build security safeguards into device designs "because we know that these risks have affected other sectors and health care is not too far behind them," Fu said.

'Ingredient List' Could Prove Helpful

He also addressed several other developments that may help shore up the cybersecurity of medical devices. These include efforts to make more information available via a software bill of material, which is "basically an ingredient list of third-party software on the inside of a medical device," Fu said.

This would help hospitals and other users "better understand risk management" for the device, Fu said. Related activities also address procurement of devices, so that a health care delivery organization can be assured that "what they are getting is what they expect." He called this "a very active space." So far there are "the beginnings of documents being written," with a "very broad set of stakeholder groups" involved internationally, Fu said. The goal is to have a "harmonized" standard and "universal expectation" for what manufacturers have to provide.

Another promising area is threat modeling, which Fu likened to the "cybersecurity equivalent [of] hazard analysis." He noted that FDA issued what he called "a handy reference guide, mostly for medical device manufacturers."[3] Threat modeling addresses "how…you characterize an adversary, what you're trying to defend against, what kind of security properties…you are trying to ensure will be in place."

Don't Buy Impulsively

Yet, organizations aren't helpless. They can take steps to enhance device security now. One strategy is to ensure that security staff have the ability to make an assessment before a medical device is purchased, which may require a change in the "culture of the organization" to ensure these individuals are included early in procurement decisions, Dameff said.

This doesn't always happen. "I've seen in several organizations that procurement does not at all involve a security assessment due to the culture of the organization," Dameff said. "Often what happens is they'll need to buy a medical device. This will be prompted by a particular department…requesting a particular device."

For example, a cardiologist may say, "I like this type of machine to do my cardiac catheterizations." The purchase request "goes to a procurement team whose main preoccupation is satisfying the requirements of the clinical team," Dameff added, "and nowhere in that type of initial vetting are security concerns taken into account."

Add Security to Procurement

Dameff said his "sincere suggestion, and this can be hard," is to "reengineer the process to have an assessment… to see what the [security] posture of the device is before you go too far down the procurement pathway."

If the IT and security staff are brought in late, "it's very hard to reverse that momentum" to stop a purchase,

Dameff said. As a result, the organization might have to make "concessions to [allow for] incorporating an insecure device on the network," such as trying to isolate it or put it on an segmented network.

Ideally, "what you want is at the very beginning, before you're actually even making an exhaustive list of the types of devices you could purchase, involving security…in the process," said Dameff. "You'll save yourself a lot of headaches, and you'll also put much more secure devices on your network."

Fu also recommended that organizations join the Health Sector Coordinating Council, which is a public-private partnership that includes a cybersecurity working group. Fu said the council "has consensus documents" and that organizations "don't have to start from scratch" when looking for cybersecurity strategies. For more information, visit https://healthsectorcouncil.org.

'Cash for Clunkers'

Government funding for replacements is another suggestion Dameff discussed.

Dameff said proposals have included "cash for clunkers" types of programs, built on the idea of letting the "federal government subsidize the cost of replacing legacy medical devices." A hospital could "trade in your old CT scanner that's running Windows 7, as an example, and we'll subsidize the cost of a new, more secure, CT scanner at 75%."

This would help smaller organizations that "don't have a budget to replace their legacy medical devices," he said, and will result in "demonstrable improvements in their security."

Such a program would "require a large investment from Congress," he acknowledged.

Federal funds to support cybersecurity infrastructure is another possibility. Dameff said he and others have advocated for a "large federal stimulus" for health care security that would "subsidize, basically, a complete reinvigorating or reimagining or reestablishment of a health care cybersecurity infrastructure at hospitals."

This could be similar to the government's program via the HITECH Act of incentivizing organizations to adopt electronic health records that met certain goals. "Let's do the same thing for cyber," he said. "That would raise the water and float all boats" in the cybersecurity ecosystem, and help address legacy systems—although they are "only one part of the problem," Dameff said.

The legacy issue is bigger than it seems, said Dameff, calling the known problems "the tip of the iceberg." Yet, he said, "it's really hard to appreciate how big a problem this is and give objective numbers primarily because we in this space have very little reliable data."

When he testified before Congress in July, Dameff noted that "most hospitals are not currently equipped to measure or report the impact of these attacks. I recommend the development of standardized metrics of cyberattack severity on hospitals."[4]

Database Would Feed Research

"Mandatory reporting of patient safety and care quality outcomes should occur for severe attacks," he told Congress. Dameff also said both the National Science Foundation and the National Institutes of Health should "prioritize funding for research on this topic."

Added Dameff: "I can't tell you how many ransomware attacks have hit hospitals in the United States in the last year." There's a similar lack of information on legacy devices, he said.

Dameff also advocated for the creation of a national database for medical device cybersecurity incidents where reports of compromised machines and technology could be submitted and viewed publicly. This could "potentially" be something like the Vaccine Adverse Event Reporting System (VAERS), he said.

"What I would rather have is a very low bar to reporting and have a lot of noise that we have to go through [and] that isn't only open to people like biomedical engineers or senior management," Dameff said. "Instead, a frontline health care worker can say, 'This device malfunctioned. I'm concerned. This might have a potential cybersecurity etiology to it; please explore it.'"

If this information were made available beyond an individual affected organization, there would be "a much higher chance of catching something," Dameff said. Information about incidents is in danger of getting lost or ignored if reporting by frontline health care workers must go through "the chain of command"—and no such data is being collected or collated nationally, he said.

Besides alerting others, a major purpose of such a database would be to collect information that researchers can study.

"That's really the key," Dameff said. "The reason we don't have good data on this and why we don't have peer-reviewed articles on this type of thing is because these institutions are very siloed, and they're not incentivized to share their information about potentially compromised medical devices."

He added that organizations are not "mature enough internally to even understand when they have to report some type of malfunction to a regulatory agency, for example, like the FDA."

There are "a lot of problems [in] collecting this data and allowing a frontline health care worker to effectively report when something might be fishy," Dameff continued. Moreover, agencies should validate the information submitted and publicly report findings.

Contact Dameff at cdameff@ucsd.edu and Fu at kevinfu@umich.edu.

1 Theresa Defino, "Cyber Disaster Plans, Training Help 'Ecosystems' Survive the Inevitable," *Report on Patient Privacy* 22, no. 2 (February 2022), https://bit.ly/3tcaiRg.
2 Kevin Fu et al., "Cybersecurity Incidents – A Threat to Patient Safety and Healthcare Delivery," webcast, ECRI, January 26, 2022, https://bit.ly/3HyP2LA.
3 MITRE, *Playbook for Threat Modeling Medical Devices*, November 30, 2021, https://bit.ly/3pEr1vA.
4 Christian Dameff, "Testimony of Dr. Christian Dameff MD Before the Committee on Energy and Commerce Subcommittee on Oversight and Investigations U.S. House of Representatives, 'Stopping Digital Thieves: The Growing Threat of Ransomware,'" July 20, 2021, https://bit.ly/3rw1QN4.