COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 4. April 08, 2021
As Pandemic Enters 2nd Year, CISOs Face Ongoing Telework, Telemedicine Challenges

By Jane Anderson

As the COVID-19 pandemic progressed from its urgent beginning to almost a "new normal," chief information security officers (CISOs) at health systems have been fighting to combat emerging cyberthreats while supporting the sudden shift to telemedicine and working from home. In doing so, the officers said, the experience offers lessons for the path forward.

Five privacy and cybersecurity experts offered their take on the pandemic and what it revealed about the health care industry's cyber strengths and weaknesses on March 22 at the 30th annual National HIPAA Summit, which was held virtually.[1]

"Last March was a pretty big blur," said Jacki Monson, vice president and chief privacy and information security officer at Sutter Health in northern California. "Literally from one day to the next, we went from having a couple of hundred workforce members working from home to close to 15,000." This affected security, of course, but it also affected workflow, she said. "Things are different with people working in the office versus at home, and there's lots of security issues and lots of privacy issues that we had to accommodate."

Telemedicine was a major, urgent issue, Monson said. Prior to the pandemic, Sutter Health had some telemedicine activity, but when California canceled all inpatient and outpatient appointments in March, the health system had to move as many appointments as possible to telemedicine, she said. "We went from about 400 or 500 telemedicine visits to close to 200,000 a day within a couple of weeks when the pandemic hit, and there's all kinds of challenges and opportunities that came with that with respect to security."

HHS helped by issuing emergency public health exceptions that allowed providers some flexibility with telemedicine early in the pandemic, Monson said. But the health system still had to select and implement telemedicine platforms, all while the pandemic was building, she said. At the same time, "we also saw the cybersecurity numbers of potential attacks triple. And so it was just a very, very busy time trying to manage it all."

Monson said that her team did not experience any furloughs. However, many workforce members in field offices, hospitals and clinics did, "because obviously, when you close operations other than inpatient critical functions, you have a lot of workforce members that you just don't have work for." Bad actors seemed to realize this dynamic existed, she said. "We actually had some individuals approached at one of our affiliates to sell their user name and password for around $20,000 to give [the bad actor] multifactor authentication access to our systems." There also were issues surrounding access to COVID-19 research data, she said. "So I'm not sure we could have run with a smaller staff, and we have been very fortunate not to have been impacted by any layoffs or furloughs, just because of the criticality of the function. And we really believe that privacy and security is a patient safety issue, and so that's how my senior leaders contemplate needing to continue to invest in it."

Darren Dworkin, senior vice president of enterprise information services and chief information officer (CIO) at Cedars-Sinai Health System, said it moved rapidly to ramp up its telemedicine operation. "We went from a rough utilization of 3% to 5%—which parenthetically we were awfully proud of—to breaking 50% and 60% in some areas," he said. "It was an interesting time to be a CIO. Our first reaction was to support our frontline caregivers and really figure out how to support our patients and our community by essentially saying 'yes' and being as flexible as we possibly could in ways that, candidly, we didn't really imagine we would do. The truth of the matter is that sometimes an emergency drives in necessity."

Still, Dworkin added, "very quickly it sets in that there does need to be some degree of hardening. To be perfectly candid, we're still dealing with that aftershock of what that hardening looks like. Some of those things just take a really long time." As the pandemic moves into its second year, it continues to "essentially affect all of our operations in ways that we didn't really understand" during the system's quick initial reactions. He said his team is still trying to figure out how to handle some issues.

Remote Work Was Top of List

As the pandemic began, Gary Gooden, CISO at Seattle Children's Hospital, said that he realized almost immediately that a large part of the hospital's nonclinical workforce would be sent home to work, and so he needed to determine "how do we protect our remote connections? It's as basic as that." Seattle was one epicenter of early pandemic activity. Of course, to protect those remote connections, the hospital had to secure multiple home office connections, he said. "That, in conjunction with the hyper-increase in the threat landscape only served to exacerbate what was already challenging in cybersecurity."

Seattle Children's rapidly implemented a remote work program, Gooden said. "We have a percentage of our employees today who are permanently remote workers. We have a subset that is hybrid. And then, of course, you have folks who simply have to be on premises through the health system—and when I say 'health system,' I'm talking about Washington, Alaska, Montana and Idaho." When roles shift, as they did during the pandemic, technological entitlements shift as well, he said.

"This, to me, is a provisioning issue" when adding, moving, or changing personnel in terms of their roles, he said. "What we have seen is the opportunity to further automate the entire provisioning process, as opposed to having somebody move into another role manually, and their inherited rights are maintained when they should not be." Seattle Children's program, "as it exists today, is fairly robust," Gooden said, "and what we're going to be doing over the next year or so is to really focus on more automation."

CHIME Had Early Warning

Russ Branzell, president and CEO at the College of Healthcare Information Management Executives (CHIME) in Ann Arbor, Michigan, said some of the earliest phone calls his organization received originated from northern Italy. "They were telling us what they were seeing, and it wasn't very many days afterwards that we started hearing about it in Seattle and in New York." Branzell described the situation as "a two-front battle" that involved coping with the pandemic's effects and battling a vastly increased number of cyberattacks simultaneously.

"Everyone was already battling on the front of digital health and moving as fast as almost every health system could possibly move," Branzell explained. "It didn't matter if you were the tiniest critical access hospital or you were the biggest academic center—everyone was moving down a path that was already stretching almost all their resources to the very edge. And then this pandemic occurred, and what happened was the speed in which they were already going—maybe too fast—accelerated to a pace that almost none of us could have ever projected nor have ever even thought of. If you had projected that a month before this happened, you would have thought everybody was crazy." From a cybersecurity perspective, he said, "it really consumed all available resources" to a degree he thinks no chief technology officer, CISO or chief information officer has ever experienced.

The second "front" came as a surprise, as cyberattacks increased as much as tenfold, Branzell said. "Not only did we send everybody home—all of us did—every home became a point of security threat. And, it wasn't just for telemedicine, even though that's huge. It wasn't just for remote monitoring—that's huge too. The reality is, every end point computing becomes a threat to an average health system or hospital or medical group or whatever the health care environment is. So the standard now for all of our members is every device anywhere in the world needs real-time access securely, which is an impossible standard across the board."

"That's the end point piece I can relate to, where we now have to worry about Amazon Echoes, Google Home, you name it," Monson added. "Even the 12-year-old wannabe hacker that's one of the kids of our employees—all of those factors now play into how we have to protect our expanded perimeter, which I think is challenging. And then the other piece to that is, even if we know how to solve the problem," there's not always technology available to solve it in an easy way.

Threats Rose With Virus

Cyberthreats began immediately as the pandemic took hold, Gooden said, adding that the threats quickly became "exponential," and the reaction to the threats had to be just as aggressive. Throughout 2020, the threat landscape was related to the pandemic, but it also became intertwined with threats and scams related to the 2020 election, he said. Nick Culbertson, co-founder and CEO of the security firm Protenus, agreed that the elections created an influx of activity in October and November that added to the increasing trend of data breaches.

As 2020 progressed, the threat landscape became more extreme, with extortion from hackers growing, Monson said. "Obviously, we want people to feel safe to get their care," she explained. "A lot of times, they're sharing their most sensitive information with the health system. And so the idea of that becoming public, or the threat against us to make that public if we don't pay a ransom, is a really challenging environment that I didn't necessarily see coming as quickly as it did."

"We've had to accept a lot of risk around technology, given the pandemic and needing to move rapidly to accommodate the needs," Monson said. For example, COVID-19 vaccines are being distributed in California by Blue Shield of California, which selected a different technology than the electronic medical record that Sutter Health uses. Therefore, "we've been working through the risks, not having the same security or privacy requirements that we would expect as a system, and making sure that everyone is on the same page around that," she said. "Being able to accommodate risk and figure out what the right level of risk is to accept has made for a really challenging environment, but at the end of the day, our job is to take care of patients and ensure their safety."

On a good note, Dworkin cited the collaboration that has occurred, in part via organizations such as CHIME, for helping his health system adapt to the rapidly changing landscape. "A couple of dozen or so colleagues that I've been in touch with from across the United States really have been the foundational reason why we've been able to adapt and be as agile as others have perceived us to be, because we were able to get some insights into what was coming. My hope is that these natural networks that got created between people are one of those everlasting sorts of silver linings. I think we're going to be able to build on the collaboration." Dworkin added, "Wherever there are opportunities for collaboration, seek those out."

Gooden agreed: "Being an information sponge and being an open collaborator is, to me, critical. The wave of collaboration that was heretofore unseen should be the new normal. Anything else, in my mind, would be doing a disservice to our respective communities."

The speakers listed several resources for organizations seeking cybersecurity help. The federal Cybersecurity and Infrastructure Security Agency is a great resource, particularly for smaller health care organizations, Monson noted.

CHIME's annual cybersecurity survey has found that "everyone is getting better at cybersecurity," Branzell said. In fact, the survey uses a standard that increases every year, so "as everybody continues to improve in their overall scoring...they're improving against an ever-increasing standard." However, smaller organizations that don't have as many resources are not advancing in their capabilities as quickly. "And so what we're seeing over the last three years, in every single area, without exception, is that there is a greater and greater divide between the haves and the have-nots," Branzell said. "We've got to figure out how to help those people in those organizations." One potential way to help is for larger organizations—the "haves"—to build up an organizational structure that can offer services to the "have-nots," Gooden said.

Regarding the future, Monson said she is wondering, "When does the emergency go away? Some of the public health exceptions that I think were great to start with and maybe are now challenging to us, particularly for deploying new technology—at what point do we just operate in the new norm and do some of those emergency exceptions go away?" She noted that her vendors have been experiencing constant cybersecurity issues, mostly as a result of "not having basic cyber hygiene." That's completely preventable, she said. "And so I would like to see standardization around cybersecurity, not just for covered entities, but for business associates and vendors who operate in this space to have some more teeth around basic cyber hygiene to get them all on the same page with the rest of us to hopefully mitigate some of those breaches."

Gooden said he doesn't see the security threat landscape improving anytime soon, because for bad actors, "it's a good business for them to be in." Therefore, he said, "the regulatory practices and the practices that the various organizations have to have in place for themselves, to protect your environment and ensure this information is safe, are critical." Still, he said, "think of security from a 360-degree perspective. Every single potential threat vector is an issue, but at the same time, you don't want to be seen as a group of 'No.' You have to be seen as a group of, 'Yes, how can I help you? Let's try to figure it out securely.' And if you think of it that way from a philosophical perspective, and if you have the kind of support that you need to have from your board and from your executive suites, you're going to be in a much better place. That's my basic thought process."

[1] Russ Branzell et al., "Lessons Learned from Emerging Privacy Data Threats during a Pandemic," The Virtual Thirtieth National HIPAA Summit, March 22, 2021, https://bit.ly/3mlVuf4.