4sight Health Roundup Podcast
March 7, 2024

David Burda:

Welcome to the 4sight Health Roundup podcast, 4sight Health's podcast series for healthcare revolutionaries, outcomes matter customers count and value rules. Hello again, everyone. This is Dave Burda, news editor at 4sight Health. It is Thursday, March 7th. We ended last week's show by mentioning how the cyberattack on Change Healthcare could cripple much of the healthcare delivery system. Today we're picking up where we left off as the industry assesses the current and ongoing damage. To share their lessons learned from this unprecedented attack are Dave Johnson, founder and CEO of 4sight Health; and Julie Murchinson, partner at Transformation Capital. Hi Dave. Hi Julie. How are you two doing this morning, Dave?

David W. Johnson:

Well, I'm feeling pretty smart, Dave considering that the cyberattack on Change was my big item from last week. And here it is, the mainline event. Nothing better than that. Really.

Burda:

Yeah. Yeah, you called it. Julie, how are you?

Julie Murchinson:

Yeah, listen, I'm just hoping that President Trump can help us develop a better relationship with the Russians, so we stop getting hacked like this because it's ridiculous. <Laugh>

Burda:

<Laugh>. Ouch. that can go all kinds of different ways, we'll just leave that there. Thanks Julie. Alright, before we talk about the fallout from the ransomware attack on Change Healthcare, let's talk about your cybersecurity experience. Dave, have you ever been victimized by some sort of cyber attack, identity theft, or someone breaking into your social channels?

Johnson:

Identity theft when I was in graduate school. You know, I suffer from the curse of a common name, right. David Johnson. How many of us are there in the world? I mean, way too many. And anyway, somebody used my name and address on an electric bill and you know, it took a while to straighten out. And after we moved to Chicago, I got a call from the Illinois Department of Family and Services, wanting to know if I was the father of a couple of kids. But, you know, those are analog crimes or <laugh>, you know, identity theft in an analog era. Pretty easy to straighten out, a whole order of magnitude difference today.

Burda:

Yeah, yeah agree. Thanks Dave. Julie, how about you? Any experiences with [00:08:00] cyber attacks on your computer? Identity credit card accounts?

Murchinson:

We had an identity theft issue in our family about a decade ago that wreaked havoc with the IRS. That was super fun. And then I think I get hack attempts in my email almost every week about Facebook. I mean, you know, it's everywhere.

Burda:

Yeah. It's a constant barrage. Years ago, and I guess this is in the analog era as well, a person started posting nasty comments and racist statements on media, website comment sections using my name. I didn't know about it until this columnist at the Chicago Tribune called me up out of the blue to verify what I allegedly said and if I really wanted him to print what I allegedly said. And I told him that I didn't. And I didn't know what he was talking about, and he didn't believe me. And that started a long trail that led to a public relations person that I had apparently pissed off as a reporter. No surprise there, but I guess this was his way of getting back at me. It was pretty nasty business. So Yeah. Yeah, it was pretty crazy. Well, this Change healthcare situation certainly has turned into nasty business. Let me give you a quick recap. On February 21st, Change Healthcare was hit with a cyber attack in the company which United Health and Optum bought in 2022 for nearly $8 billion, shut down all of its health IT systems for what it expected would be a day or two. On February 27, Change said the shutdown could last weeks and it set up a temporary loan program for providers who can't get their claims paid through changes payment systems. On February 29th, change confirmed that it was a ransomware attack from a threat actor called Black Cat. On March 1st, media reports said Change paid a $22 million ransom in Bitcoin to Black Cat to unlock its health IT systems. And on March 5th, HHS announced a list of steps to help out, including expediting requests from providers to change claims processing clearinghouses. All the while hospitals medical practices and pharmacies aren't getting paid, patients aren't getting prescriptions filled. The American Hospital Association is involved, the American Medical Association is involved. It's the very definition of a cluster. Dave, there's a lot to unpack here, but give me your two or three big economic or policy takeaways from what happened.

Johnson:

First, this is clearly a major crisis. I agree with the hospital association executives who are saying the most significant cyber attack on health in US history. Shoot, it might be the most significant cyber attack on the US period. It's that large. The private industry response by United has been wholly inadequate. So that's point number two. They're clearly making it up as they go along. I read about one large primary care practice in Pennsylvania with half a million dollars in unpaid claims. And United offered them a $4,000 loan. So coverage on less than 1% of what the, what the cash flow problem was. Well, that's not gonna do it. And I'm halfway wondering if United or Change is gonna go after the government to reimburse 'em for the 22 million that they paid in ransom. So where does that leave us? Like always that in times of major financial crisis, the government needs to ride to the rescue. It's yet another heads eye win tail, you lose type of situation. And so we’ll get through this and sort of my question is then what do we just wait for the next one or do we actually do something about this? That will be interesting to watch. But what I find myself thinking you know, in typical Dave fashion is I'm looking at the bigger picture and asking why our healthcare baby is just so damn ugly. And why is it subject to these types of attacks? And I think it all comes down to basics. You know, payment, first care second, operating model, differential pricing for identical services. An open invitation to payers and providers to manipulate the payment system for their own benefit. You know, as long as they don't cross too many lines. The entire lack of transparency and, and pricing even for routine things, a trillion dollars. And we've talked about how big a trillion is. A trillion dollar revenue cycle business with no real public accounting of how big it is or what are the different components or so on. And I think all of this way of thinking this, this money first mentality reveals that healthcare soft underbelly is just ridiculously open to attack. It's something like 30 to 40% of all cyber attacks are on healthcare organizations. So can we blame the Black Cats of the world and the other cyber criminal gangs for targeting healthcare? I mean, I don't like it, but it feels like we're an easy target.

Burda:

It is true predators go where the prey is, and healthcare is the the prey right now. Thank you Julie, any questions for Dave?

Murchinson:

So Dave you had a cyber attack relatively recently in Chicago at Lurie Children's. Right? So my understanding of that is that the, they were down, epic was down for a long time. What, what was going on there?

Johnson:

Well, a different cyber attack gang, but you know, the same M.O. And they got into the EHR at, at Lurie Children's, And almost everything stopped, right? They had to set up you know, call centers for patients to to get their prescriptions, to figure out treatments and so on full hands on effort. And just in the last week, they've gotten their electronic health record back up and going. MyChart still isn't working. But it just shows the, the magnitude of disruption that these systems or these, these criminals can unleash. And so here you got Epic and Change two pretty big players both showing that they're vulnerable and so I, it's, it's gonna keep happening until we figure out a way to stop it.

Burda:

Now, Julie, I can't see you, but I read your mind when Dave said MyChart didn't work and your thought bubble said, did it ever work?

Murchinson:

<Laugh>, Dave, you know me too Well. Yeah,

Burda:

Yeah, I got that one. All right, Julie.

Johnson:

I heard the chuckle. I did hear the chuckle.

Burda:

<Laugh>. All right. It is your turn now. Julie, give me your two or three big market innovation or technology takeaways from this situation.

Murchinson:

Yeah, well, the reality is that healthcare organizations, providers specifically, have become increasingly susceptible to security and compliance issues, as we've talked about. And it's really putting patient privacy and security at risk, right? It's all about us at the end of the day, even though a lot of it's been focused on money. And while Change isn't a traditional provider, they themselves, you know, were built a long time ago, their technology may be really old and their linkages are quite unprotected. I actually did read somewhere that Elevance and maybe a couple others you know, immediately cut off their connections to Change. And many more have done that, obviously. So that just shuts down the whole system because their switch and, you know, the health systems themselves notoriously underspend on privacy and security and you know, compliance technology to even make sure that things are being done much less, you know, monitoring for big, massive issues like this. And it's not like the technology to protect data or monitor issues doesn't exist. So, okay, not to make excuses, but it hasn't been that long that we've thought of healthcare data as digital and at risk of these kinds of attacks. <Laugh>, like, even though that sort of sounds ridiculous, but this does come down to another area that is expensive and doesn't always rise to the top of the priority list. And we may not have as much sophistication in these areas as we should. And it all leads to our industry just not managing our newly found digitized data as well as other industries. And, you know, one cybersecurity firm estimate I saw is that large health systems are losing over a hundred million dollars a day. I mean, that's a stat. So I talked to Nick Culbertson, who's the CEO Pro Tennis, which is in full disclosure, one of our partner companies. And it helps health systems protect their data and frankly protect patients through their compliance analytics platform. And they're about to launch their 2024 Breach Barometer which shows that at least 171 million patient records were breached in 2023. Lemme say that again. 171 million patient records breach in 2023 <laugh>, mostly due to ransomware attacks, you know, by clap or this black cat, or, you know, like big ransomware groups. And it's a huge increase in 2024. Looks like it's gonna be worse. So that's not great. And pro tennis is actually really seeing, as, I think we all are [00:19:00] a very positive feedback loop with these cyber attacks. The more successful the breach, you know, the more we're gonna see more attackers attacking. So what's interesting about their perspective is that hacking, like this gets all the press, but their data actually shows that insider breaches are on the rise as well. So while most patient records are breached by hackers, 93% of incidents reported to HHS are from insiders, 93% from insiders. So it's coming from all angles, frankly. And what's kind of scary about it, I had a little bit of a flashback to the Silicon Valley Bank weekend. You know, we're starting to see companies, not just our portfolio, but like all over the place questioning how lenders would, you know, allow draws on credit facilities when a massive threat like this happens, right? So companies are asking weird questions about, you know, basic financing that is caused by this. So it just, it starts to throw doubt and concern in places that, you know, are the foundation of how we're, you know, we're building these companies.

Burda:

Yeah. Tremendous ripple effect. Thanks Julie. Dave, any questions for Julie?

Johnson:

A cyber attack of this type and magnitude is/ was a completely foreseeable risk; why aren't there any fail safe mechanisms in place? You know, after the financial crisis of 2008, 2009, the government forced the major banks to undertake a severe stress test to guarantee their solvency when the markets went the wrong way. Should HHS consider imposing similar stress test mechanisms on these major interfaces for medical claims and medical data, you know, like Change, like Epic. So Julie, you're the healthcare czar for a day. What do you do to make sure this type of breach never happens again?

Murchinson:

Hmm. Well, first your description reminds me a little bit of covid, right? Yeah. We all asked ourselves, why did leaders not have this worst case scenario in their playbook [00:22:00] and know how to react, react more immediately, right?

Johnson:

Yep.

Murchinson:

So your comment about how United is being accused of slow action you know, it resonates with people's concern about the situation and honestly, you know, health systems and the tech companies that serve them, whether the large ones like Epic or the small ones like we work with. If they don't take more of a leadership role in really measuring up to the way we think about other types of data and how companies protect other types of data in our lives, then the feds are gonna come in and do this, right? There is no doubt about it. And regulators are putting on more pressure, you know, recently and <laugh> right now, but I don't, I, you know, it might be too late. I mean, it takes a long time to get some of this stuff in place. So I, unfortunately, I think this is a place where government is gonna have to put some, some rules in place, which will drive up the cost of care delivery in our system and everything, and take time and, you know, be a burden, frankly.

Burda:

I'll just add that I did read that Change announced that it's building a quote parallel network environment close quote, and they want to have that up this week while they rebuild their data center and restore applications and services. So I guess it's like, what, making a second ham for Easter after you burn the first one,

Murchinson:

<Laugh>. Right. It's gonna be a better ham, though.

Burda:

Yeah. So good. Okay. It'll be the best ham ever. Thanks Julie. Now let's talk about other big news that happened this past week. Julie, what else happened that we should know about?

Murchinson:

Well, I saw a quick article in Kaiser Family Foundation about a whistleblower issue that Aldaye is dealing with, where they're being accused of Medicare fraud, which, yikes. I mean whistleblowers are everywhere. Can't believe what you see, but I'm having a hard time imagining that a company started by someone who actually knows what they're doing, wouldn't be in a better position than that.

Burda:

Right, right. Yeah, we'll definitely keep an eye on that. Thank you. Dave, what other healthcare news blipped on your radar this week?

Johnson:

Well, you know, I'm on the new book, and Paul and I got the first half into our publisher, Wiley, on Monday, so major event. But the reason I mentioned it is as this was happening Paul's gallbladder blew up, and so he's had to have some surgery. And then now he's on bedrest for a couple of weeks but never one, not to make lemonade outta lemons. He's like dramatically amped up his editing time. And so we're being more productive as a writing team than we ever have up to this point. But anyway, we're thinking about Paul and wishing him a speedy recovery and which I'm sure will happen. And the book is book is, is out there and and we'll get into the public sometime later this year.

Burda:

Got it. Well, we do wish him well. Thank you. And thank you, Julie. That is all the time we have for today. If you'd like to learn more about the topics we discussed on today's show, please visit our website at 4sighthealth.com. And don't forget to tell a friend about the 4sight Health Roundup podcast. Subscribe now and don't miss another segment of the best 20 minutes in healthcare. Thanks for listening, I'm Dave Burda for 4sight Health.