HEALTH CYBERSECURITY

VIDEO TRANSCRIPT

Presenter: Welcome, everyone to today's AHA Leadership scan on navigating the Healthcare cybersecurity storm. Strategies for Resilience and Risk reduction.

Today's event is made possible by our sponsor, Accenture. Accenture helps its clients meet the essential expectations that every person has of healthcare, of the healthcare system, access, experience and outcomes.

Today's event will feature a panel discussion featuring leaders in healthcare tech who will share impactful strategies to reduce risk.

The discussion will be followed by a Q&A. Please submit your questions and we will field as many as time allows. Following the event, you will be eligible for one ACHE credit. We will send information on how to get a certificate for ACHE credit and our post-event communications. Let me briefly introduce today's speakers.

Let's S... Excuse me. Less Stoltenberg is vice president and Chief Cybersecurity Officer at the University of Texas MD Anderson Cancer Center. Sunil Dadlani is EVP and Chief Information and Digital Transformation Officer at Atlantic Health System. Adam Zoller is Chief Information Security Officer at Providence. Kelly Summers is the former senior vice president and Chief Information Officer of Valleywise Health. He now serves as a consultant to healthcare organizations. Amit Gaur is Managing Director and Health Security Lead of Accenture. And now I will turn things over to our event moderator. John Riggi is vice president and National Advisor for Cybersecurity and Risk for the American Hospital Association.

John R: Thank you, Jennifer, and thanks to everybody tuning in today.

I think we're going to have a great discussion today. Very fortunate to have such leaders in cybersecurity joining us today.

These are our panelists today are some of the most respected and accomplished chief information officer and chief information security officers, cybersecurity experts in the country. So really privileged, for them to be here with me today on the panel.

It really at this very crucial time in the cybersecurity field, we all know as practitioners or members within healthcare, whether you're a clinician, executive leadership, or on the operations side, how much cybersecurity attacks against our hospitals and health systems have increased over the past couple of years.

Last year, a record-breaking number of cyberattacks resulting in the theft and compromise of the healthcare records of 136 million individuals.

.

That is a fivefold increase from 2020. And most concerning our the increase in these high impact ransomware attacks, which disrupt and delay healthcare delivery, resulting in a risk to patient safety.

The government has heard us loud and clear, whether it's directly dealing with the leadership of FBI, Caesar, HHS, the White House, Up on the Hill. These attacks are not just data theft crimes. These are threat to life crimes. And we're not going to be able to solely defend our way out of this problem. We need more support from the government to help go on the offense and more support in terms of human, financial and technical resources.

Big changes we have been seeing perhaps really forecasting in 2024, unfortunately, are the high impact attacks against mission critical third-party technology providers, service providers... [broadcast glitch] ... the prime example in February is when we had the Black Cat russian-speaking ransomware group attack Change Healthcare, subsequently followed by an attack against the blood supply series of attacks result culminating in a very significant supply attack against a blood supplier, for the state of Florida and southeast in July, which we had been forecasting and warning about.

When these attacks occur and I think some of the best lessons learned from these issues, from these incidents are that for us, as the end users of these mission critical third-party services and technology and supply chain is to really think about who do we depend upon for these life critical, mission critical, and business critical services? And what would be the cascading effect if these services suddenly went dark, even for non-malicious reasons, such as we saw in the CrowdStrike incident, folks were not able to predict, of course, how that flawed update eventually resulted in the blue screen of death appearing on 8.5 million computers globally, resulting in grounded planes. And more importantly for us, from our perspective, significant disruption of patient care, ambulances being diverted and, surgeries being canceled.

So, we're doing our best, as a field to try to help defend against these attacks. But more and more, we need to focus on resiliency, resiliency and recovery and trying to predict, what the effects would be, the cascading effects would be of these attacks.

The government has been giving us quite a bit of scrutiny as a result. And again, we continue to loudly and publicly advocate on the fields behalf that, again, we can't do this on our own. We need better security technology. We have to implement all the basic cybersecurity practices. And again, we need the government to do more on offense.

With that, I'd like to turn it over to our, host, Amit Gaur from Accenture, who also has a national perspective. Accenture does a lot of work with hospitals and healthcare entities across the country. And, Amit, could you tell us a bit about what you're seeing, your assessment of the healthcare cybersecurity landscape would be, is, and how, in your view, are cybercriminals changing their strategies and tactics?

Amit G: Thank you, John. Thanks for asking a great question. Healthcare security is very close to my heart and we all have seen what recently trends are showing. We all have seen a dramatic rise in attacks on healthcare, clinics, healthcare systems in past few years. You mentioned about fivefold since 2020.

The recent one of the recent report talks about healthcare grew. The cyber-attack in healthcare grew was basically the ransomware by 45% in last year alone itself. We talked about some of the examples, like [INAUDIBLE] and or even the blood bank.

It's quite clear that threats are evolving much more rapidly in both in terms of scale as well as sophistication. So let me talk about some of the things first of all, in terms of scale.

I think one of the things which we are seeing is, is an increase in attack surface with the rise of telemedicine, digital transformation over reliance on connected systems that increased from EHR to connected devices, including wearable devices

I think it's quite obvious more system means more vulnerabilities. So that's one of the key area.

The second part of it is healthcare continue to be a prime target due to high value data for political and financial gain. This is also visible in terms of price of healthcare data on dark web.

We continue to see challenges or underinvestment in terms of technology, healthcare organizations. Basically, providers continue to have challenges in terms of margins and profitability and cost and continue to depend on legacy systems, including some of the IOMT which lacks adequate security protocol, make it easy for bad actors to attack. And the last one and then the similar way is supply chain vulnerability.

You did cover some of those. I think healthcare systems are vulnerable to the supply chains. Big time record of dependance on software and services, supply chain provider, which often involves third party vendors with weaker security controls also. So, I think these are the four things which we are seeing from a scale perspective. Coming to the second part of the question, specially about the tactics, sophistication. I think in today's world, cyber criminals are running much more organized industrial... or can say it [INADUDIBLE] actually, for we are seeing terms like ‘Cybercrime at the service’, ‘Ransomware in service’. And they are leveraging more sophisticated tools and technology like Gen AI, AINML for targeted phishing attacks. Rise of deepfakes and social engineering attacks.

You did cover some of the insider threats, and I think that's one of the biggest challenges which we are seeing recently, especially some of you might have recently hear about the news where some of the nation state actors are planting operatives in key industries. These insider misuse, trusted access or even providing privileged access to the wrong people. Recent. One of the accidental insider attack is CrowdStrike, which clearly exposed how much we are dependent on technology and how much we all need to think about not only protect, but on resilience and recovery. I think those are the some of the trends, John, which we are seeing in the industry, and I'm sure we all are going to discuss more further on those.

John R: Thank you for that, Amit. And you raise a very good point here that not only are we dealing with cyber risk as a technology risk as, but it is truly an enterprise risk and a strategic risk, a risk that comes to us from outside the boundaries of our enterprise, like geopolitics.

What we see going on here with Russia and Ukraine at the moment, Russia is not cooperating with the federal government at all to put a stop to these ransomware groups that are Russia's providing safe harbor to China, very active and aggressive in planting, as the federal government has warned us of destructive malware on our critical infrastructure. See the situation in Middle East literally exploding. How will that create potential risk for us, as Iran perhaps would seek to employ cyber weapons not directed at us, directly but again, could there be an errant cyber weapon that spreads through the internet that ultimately, we become collateral damage? North Korea, Iran, all the all the usual suspects.

As I always say, Sunil, maybe I see you up on the screen right here. If I could go to you and then I'm going to go over to Kelly and then over to Adam.

Sunil D: Thank you. John. And, I will try to build on what Ahmed said. And, and you very eloquently said about how geopolitical is shaping up the cyber warfare, the way we are seeing is and I'm often asked within my organization and outside also: Are things going to be back to normal? And, do we go back there where there is more sanity? And the true response is, you know, there is no no new level. You know, there is no new normal. We are going to always see every day, every minute, every month. We are going to see more and more of this. It's just about changing our attitudes and finding out that, you know, we need to move away from reactive mode to proactive mode. I think that is the most important part.

And you said it very correctly, that no single entity, whether it's private sector, nonprofit or our public sector or federal agencies, they cannot they cannot do it on their own.

You need a national and an international coalition to really defend yourself correctly. And one of the most key part is the education within the organization. When we talk about cyber security, we always think about technology security. It's a technology problem. You really need a top, top-level support and understanding.

And we are very fortunate that we have Brian [INAUDIBLE], our CEO, who's a champion not only for the organization but for the healthcare sector. You know, he participates with federal agencies, part of a system. And, you know, collaborates with you on all the federal agencies where he has made not only patient outcome, but patient safety as a as a core part of our mission and where we are seeing now things are changing, is leveraging AI. AI has really changed the game for the nation, cyber actors as well as for us.

So what we are seeing is completely automation, you know, less human intervention.

Now people can do whatever nefarious activities they can do just with the with the use of technologies. And these are some of the technologies that are available open source or through commercially available technologies. They are all available to everybody. And we always keep reminding ourselves that, you know, all it takes is one wrong action, whether intentional or unintentional. And it can it can cause havoc to patient outcome and patient safety.

So what we are trying to do is also, you know, getting into an offense mode in terms of changing our posture, you know, layered posture, staying up to date, removing and modernizing legacy applications as fast as we can with the constraints of, of course, the financial pressures and the operational pressures and top priority being, of course, providing care to the patient.

So, it's a very interesting, game, which we, I, you know, really define us AI offense versus AI defense in the, in the cybersecurity realm.

John R: Thank you for that. Really, really sage sage advice there again to people. Right? Regardless of what we do on the technology side and we have bad guys social engineering our help IT desk bypassing phishing resistant email.

I think I said I'm going to go to Kelly next. Kelly, same question: What are you seeing out there in the threat landscape and strategies and tactics? How the bad guys changing?

Kelly S: Yeah. Thanks, John. You know, I have to tell you, I was having a conversation last week with somebody, that I worked with about 25 years ago in the pacemaker business. So, I used to be in pacemaker manufacturing. And if you remember the show 24, in the early 2000, I lived in Los Angeles, and we were actually reached out to by the showrunners of that show. And if you remember, they actually simulate an assassination by hacking into a pacemaker for a political candidate. If you remember that old Kiefer Sutherland show and, you know, we were having this conversation about, you know, the threats surface up now, right? Reality mimicking art.

You know, that was over 20 years ago. We had those kind of hyper hypothetical, ‘hey, could this really happen with a medical device?’, and now look where we're at today. So absolutely, you look at the threat service from again, perimeter medical device all the way to an implanted device.

That whole supply chain and threat surface, it's all interconnected. So I think that's what we're we're all talking about. So, then it becomes what are those techniques that I can do that threat assessment, the most likely, you know, vectors of attack of compromise, you know, from the clinical care side.

And then also from the business side, I was one of the unfortunate, participants in the Kronos, you know, human resource attack a couple of years ago. And that was right in the teeth of Covid, where we're trying to keep nurses paid, employed, working overtime, and we had to scramble to make sure that we could time track and pay our employees. So, you know, again, it's not just the clinical side, incredibly important from a patient safety, but it's really business operations. And, you know, we've talked about business continuity. Use the term clinical continuity. I think both of those are really, incredibly important, landscapes to stay abreast of for sure.

John R: Yeah. Kelly, thanks for that. That's a great point. As often as you said, we're focused on the medical debatability of medical technology. And and there's another embedded point. I think you made there is that our tremendous dependency on network and internet connected technology and the availability of that technology for patients... to provide patient care really creates risk when that technology is not available, or a third party is hit like Kronos.

So, folks may may recall when Kronos was hit, it actually impacted patient care as well. Because Kronos was being used for scheduling of clinical staff, they had to take clinical managers offline to schedule. So, understanding what the cascading effects of a loss of all that, mission critical technology would be.

Kelly S: And, John, if I could add if I can add something, I pulled up a document and I know we'll we'll probably talk about, you know, business continuity and business impact assessment. I pulled up a document that I used about eight years ago, just as a great example, and we had identified Kronos as a mission critical application with with an RTO of less than four hours. And we were down about six weeks. Just for context.

John R: So, Kelly, don't get me going on, on, on these claims by all these third-party providers that 99.99 uptime runtime capability, my personal thought is they're they just haven't been targeted by a determined, sophisticated adversary. I'm going to go over to Adam and then over to Less. The same question: What do you see on the cyber threat landscape? How are the bad guys, from your perspective, changing their tactics and strategies?

Adam Z: Yeah. Great question. And I'm going to build on, John, what you and Amit and what Sunil and Kelly have said.

You know, I think, you know, when I get asked the question of, you know, I get asked the same question, when are wins? When are things going to revert to the norm? You know, this is an election year

Is it just it is the pace of attacks higher than what we would expect in a normal year or is, you know, are we going to revert back to that mean? And my, my answer is often times what is normal really look like in this space? You know, if normal is, in people's minds, going back to a situation where attackers weren't targeting healthcare systems with damaging cyber-attacks, I think the answer is no.

And I would even argue that, although there was a, the perception, the public perception was there was an invisible red line on attacking healthcare systems with damaging and destructive cyber-attacks like ransomware.

I would argue that that invisible that red line never really existed in the first place, and that although ransomware attackers said they wouldn't target, patient care environments, we've been seeing targeted attacks against patient care, systems against against our healthcare system, since well before the the quote unquote red line was dropped, recently. And, you know, I fall back to, I guess you know, IT strategy. You know, I always say IT strategy is business strategy.

So, if we look at the attacks that we're facing, the cyber risks that we're facing externally, you know, we have to really look at cyber risk as just part of business operating risk. And when I look at the threat actors specifically, we're getting targeted by the entire spectrum of threat actors at Providence, everything from script kiddies in their mom's basement, in Russia, all the way up through sophisticated cyber criminals that are really utilizing nation state level tactics to get into our ecosystem. And I think it was Amit that said, this is a well-organized, well-oiled machine, well organized, well-oiled supply chain of cyber-attacks that's hitting, Western organizations. You know, everything from the people who create the malware to the people who then sell that and supply it to access brokers, and then the access brokers that supply access to ransomware attackers and their affiliates. It's ahh it's a well-oiled machine. And these attackers, they're getting more brazen too I know, there's been lots of reports recently of ransomware actors, researching executives from organizations that have been hit by successful ransomware attacks, figuring out where they live, and even hiring people in their localities to go and take photos of their families or photos of their children in school and say, hey, you know, what are you going to do if we target these people with attacks?

You know, here's your family, we know where you live, etc., etc. to get them to pay ransoms. And so again, I think unfortunately these attacks are going to continue, until there's much more real consequences, that these attackers face. More direct consequences that they face beyond just confiscating cryptocurrency and shutting down their command-and-control infrastructure.

So, I always fall back on, you know, as a CSO, what can I do? Understanding that the attack surface and the threat actor the threats face is going to change. The attack surface is going to expand as Amit noted, you know, focus on what you call I set strategy aligned to my business and understand what the business is trying to accomplish and reduce risk on their business operations. And I use my seat at the table to be a strong voice for reducing cyber risk. And really, an educator as well on teaching, what are the changes in the industry? How are those threat actors evolving and what do we need to do? What do we need to invest in to stay in front of them?

John R: Yeah. Great points, Adam, especially your point about that red line. That invisible red line. Yeah. I don't know if folks recall, but at the onset of the pandemic, there was a particular Russian ransomware group. I can't recall the exact name.

One of the major groups said we will basically have a truce. We will not attack healthcare due to the global, health emergency that lasted about a week and a half. And, before the other groups just saw that as an increased opportunity to make to make money in to your other point, how they're pushing the boundaries.

I've been involved in ransomware negotiations, helping hospitals during those situations. A couple of years ago, we could say, hey, we have ambulances on diversion, and they would sort of back off and they would say they would reduce the ransom amount. Lately they say, ‘Oh, you have ambulance on diversion and cancel surgeries?.

All the more reason you should pay quickly.' That's what we're dealing with. And to your point, we've got to impose risk and consequences to deter that behavior. Less, over to you, MD Anderson. Globally, in the global spotlight leading cancer center groundbreaking research. All types of people are targeting you. How do you keep up with that? Less. Give us your perspective on the threat landscape.

Less S: Yeah. The, I don't think that we'll ever go back to a normal. Right. I mean, they continue to escalate and continue to be more and more targeted attacks against us. Just like Adam was saying, it's everything from the script kiddies to the extremely, advanced nation state actors that are targeting us on a daily basis. I think they're also learning from, you know, the impacts of change, healthcare, Kronos, the blood supply, you know, they can impact the industry from that perspective as well. And I think, you know, I think we're going to see more and more of that and more and more kind of consolidated or, well, coordinated attacks, maybe between third parties and as well as, providers.

On the targeted side of the house, I'll give you just one example. We've got a very famous professor, scientist, where we had an attacker literally go out, find his high school counselor, that it was turning 100 years old, went out and interviewed that individual, created a YouTube page with that interview, and then contacted our scientists, basically saying, hey, I just interviewed your hunter or your counselor from high school. They just turned 100. I'd love to interview you. And our professor obviously took that bait almost instantaneously. So that's how sophisticated they are.

From a targeting perspective, both, you know, externally as well as internally. So, yeah, I don't think we're we're ever going to be back to any type of normal. And that escalation is going to continue to escalate.

John R: Yeah. Thanks. Thanks for emphasizing the point to the levels of social engineering that are going on right now, because everybody's information is out there.

So, folks want to look at our social media. You know, us in this community are not, very prominent on social media unless you're public, like myself, to be an advocate. But, the how they're buying that information again, manipulating it, manipulating help IT desk individuals. And then, as Sunil mentioned, the use of AI to accelerate these types of attacks with social engineering. I did have, a couple of first confirmed reports of deepfakes being used in conjunction with IT helpdesk just a couple of weeks ago. Amit I'm going to go back to you here now. So we hear this discussion, folks know that cybersecurity is a priority.

Every CEO I speak to, now ranked cyber risk is one of their top 1 or 2 cyber risk issues. But again, it is I remind policymakers and I make statements in the media. Hospitals and health systems are not cybersecurity companies. And even if we invest every dollar in our budget for cybersecurity, we still will not be bulletproof, in a sense, from these cyber-attacks.

So, when it comes to prioritizing investment for cybersecurity, Amit, from your perspective, how are health systems, the hospitals and health systems handling, what are the challenges they're facing to help try to prioritize cybersecurity initiatives and investments, knowing that cybersecurity is important but job one is to take care of patients and save lives?

Amit G: Thank you, John, for asking that. I think that that's a difficult problem to be solved, to be very honest, especially with the current market scenario, that everybody is facing a tighter budget, right?

The reality that threats are constantly evolving, and it's not just possible for anybody to fix everything.

So, one of the things which works very well for people is doing the right level of risk, alignment and understanding the risk, and then start focusing on targeted solution better than trying to fix everything.

That is one of the things which I have seen very recently especially see. So, the are focusing in terms of prioritizing that risk. But it's not about only protection, right? Protection is a part of it. We have to find the right balance. And that's where I think now most of the providers are start thinking about not only focus on protection, but in terms of building resilience and ensuring we can recover faster. Right? That's the most important part because it's not about if it's more about that. Right?

So, everybody there's they're much more focus now in terms of recovering, putting together of a response, incident response and those kind of tech. Right? I think the other thing, which is seen as very important and effective is working with business. Cybersecurity is no more a problem from a technology perspective. I think some of you had already mentioned it, right. Most of the CSOs now have ability in terms of board.

I think that's where they are. I've seen that people are start getting much more focused in terms of budgets and aligning those based on the priority. But according to me and what we are seeing it, it's more about balancing the available resources across different areas and not only focusing on protecting.

John R: Thank you, Amit. Sunil, I'm going to go back over to you again. Same question. What are the challenges you're facing when you, prioritize or attempt to prioritize cybersecurity initiatives? For the greatest impact?

Sunil D: That's a great question. And again, it all starts with, first of all, having a good understanding of your attack service. You know, hotspot systems try to grow organically and through the mergers and acquisitions so your attack surface is always expanding. You'll never shrinking. That's one part now within the attack surface. Should you be worried about everything and put investing investment dollars everywhere?

I think that may be a flawed strategy. You need to prioritize and identify your crown jewels in terms of your data in terms of your application that has direct impact on on your patient care, for example, ICUs, imaging labs, medication and ORs, you know, behavioral health service line, oncology, radiation.

There are some some ways where through which you have to do a ruthless prioritization because you will not be just be able to, you know, as you said, you know, bulletproof every, each and every part of the, of the attack service.

Second part is then understanding and mapping, you know, where do you have highest vulnerabilities and which type of vulnerabilities you have? Do you have legacy? Do you have third party? Because mapping third party and is the most difficult part. You know how many third parties are involved in provisioning services, what services they provide? You know, what are the technologies we are using?

What fourth party or third party, those third-party services are being used.

So, it's a complex maze, but you have to do whatever you can. And for example, as you know, as I mentioned, epic and, you know, imaging lab systems are the core systems that, and, and blood bank, those are some or, organ transplant.

Those are some of the very high, high priority areas there where you really need to focus and then, you know, look at it about we are looking at clinical side. But on the non-clinical side, payroll is also equally important. If the people don't get paid, they will not be even able to supply the to provision the care.

So even that becomes part of the core mission critical application. And this is these are some of the things that that comes into my to our mind. And it's very difficult to really map for each application what is going to be the impact, what is going to be the ROI? It's just that, you know, you have to focus on where the how do you contain the blast radius? In simple terms, I think that is the most important part, that containment and then recovering resiliency is all about how quickly you can you can stand up on your feet after taking a punch. So, these are some of the things that, you know, business continuity, incident response plan and taking those decisions. If it happens in the middle of the night, you're not waiting for, you know, bureaucracy to have ten different calls and make those calls.

You know, people should be empowered and make those decisions if they have to make those decisions. These are some of the things that, you know, that we we have our framework based on.

John R: Yeah. Great points, Sunil. And I really just want to emphasize some of the points you made. It may be, despite best efforts, almost impossible to predict the cascading effects as a result of a loss of a particular piece of technology.

Who would have ever predicted that CrowdStrike, a flawed update would result in the blue screen of death for 8.5 million computers and then ultimately ambulances, and would be on diversion and flights being canceled. So the point is, and I think everybody's made this, is to think about redundancy and resiliency, the loss of technology, for whatever reason, malicious or non malicious, or we lose the internet connection because China has planted something there that has taken down our internet.

Understanding what the loss of technology in general, trying to prioritize the obvious where you can but thinking about how do we go back to analog manual procedures without such dependency? On technology thoughts? Let me go over to, shake it up a little bit. Less I made you wait last time for the whole amount, I'm going to go to Less, Adam, and then Kelly.

Less S:

Here, yeah, I completely agree with prioritizing vulnerabilities and investing in, you know, the the detection, response, protection aspects of things.

What we have also realized from some of the tabletops that we've done is that resilience. And so we have really focused on helping educate our operations folks, how to operate without any type of digital capabilities and have done literally, you know, like five different daylong workshops where we have people, you know, check in mark patients, have them take blood work, have them do the labs, have them take, you know, get radiation therapy without any digital capabilities at all.

So, you know, really practicing that. So, you know, if, heaven forbid, that ever happens to us, you know, that they could actually still treat patients, in a very critical, setting. So that's one thing.

The other thing that I would say is also looking at the front end of things. So, when you're bringing in new technology, making sure that you're doing those risk assessments and making sure that you're not adding to the problem, with new technologies that you're bringing in, because that's a great time to basically be able to set some security parameters and architected in a way that is, both protected as well as resilient. So those are the couple of things that I would add to it.

John R: Yeah. Thanks, Less. And I know your CEO doctor Pisters, is one of the nation's leading advocates for cyber security. And, you know, just tremendous, assistance there on this issue. A patient tracers, as you said, the clinical workflow, mapping it all out, and Less, can I just a follow up question for you.

So, are you involved, from the cybersecurity side, when there is a contemplation even of or review of the acquisition of technology coming in, are you part of a committee that requires any technology?

Less S: Absolutely. Any technology that comes in. We are heavily involved. So, you know, we've got ties into sourcing and contracts are legal folks. So if they see any type of technology coming in, there's a hard stop that basically bumps it over to us to, have a review.

John R: All right. Thank you. I think I said I was going to go to Adam next. Adam, what are your thoughts on prioritization of investment in cyber?

Adam Z: Yeah, great point so far. What I would add is I'd say start with what costs very little but has, enormous outcomes. And to me, that's the culture of the organization, the tone at the top. You know, I'm blessed at Providence to have a very supportive CEO, CIO, board of directors, educating them and having that tone at the top and then communicating down that tone at the top to the business, has enormous, potential for outcomes, but cost very little. The other pieces at Providence, what we do is understanding, I think to your point, Sean, you can sink infinite amounts of money in this problem. And still, at the end of the day, if the probability is greater than zero that you're going to get compromise or deal or deal with an event, you're eventually given enough time going to have to deal with an event. And so the way that we look at this is we assume that we're going to eventually have to deal with some sort of a cyber security event, but we don't want to just trust our own analysis of how well we're performing.

So, we we conduct, maturity assessments based on the National Institute of Standards and Technology, the NIST, cybersecurity framework on a two year basis. We have an outside third party come in and assess our maturity according to that industry standard cybersecurity model, to point out where our points of weakness and where are we actually doing very well. And then we assess ourselves and gauge ourselves, not against just, the healthcare sector, because I think in large part, unfortunately, the healthcare sector lags behind in cybersecurity maturity, but we're aiming toward more mature sectors and to compete at the same level as, say, the financial services industry, the defense industrial base, and really borrow some of the best practices from those industries to advance our cybersecurity maturity.

And the thought process behind that is, again, we could sink infinite amounts of resources into this problem. And I, as the CSO, can really only focus on a handful of things at one given time. By taking that third party view and using an industry standard model, we're taking all bias out of the equation and saying: What is right really look like? Industry agnostic? And then we can then take the outcomes of that and prioritize the cybersecurity strategy on the most, the hardest hitting and highest risk items.

John R: Great practical advice, and I've got to give a shout out to your CEO as well. Eric Wexler, again, a leader very active on cybersecurity. And I think, really does set the tone, for the entire organization.

I always say that one of the fundamental pillars of cybersecurity is leadership. It's got to be a leadership issue. And, one follow up question, Adam, for, you know, when you get this outside evaluation, do you make use of really aggressive red team testing and really that really be beyond the compliance on the risk assessment? Tell us what you can do other than that without giving away too much.

Adam Z: Yeah I wouldn't want to divulge my sources and methods. But yeah, we do. And I think, someone mentioned before me attack surface management is a really important part of, defending your ecosystem from cyber-attacks.

As you know, no cybersecurity talk talk would be complete without a quote from the Art of War, right? Know yourself and know your enemy. What better way to be able to prioritize your defenses than to attack yourself using the same methods, the same sources, methods that the attackers use against you, the same tools which they use against you.

So, we do employ full time penetration testers. And full-time red teamers using red team tactics. We also, do outsource red team and pen test activities on an annual basis using a third party. Because we know that we don't have the, we haven’t cornered the best practices from a red team perspective. And that’s those are fairly expensive talent.

I also have a robust cyber intelligence team that’s looking at, what are the threat actors investing in from an R&D perspective? Who are they talking about targeting? What's going on on the dark web? Is our data ending up on the dark web, our accounts ending up on the dark web? Who’s getting targeted, and how are they getting targeted? What are the threat actors talking about?

And all those different pieces, contribute to a security strategy that’s not only looking at cyber maturity, but it’s also looking at, what are the types of threats that we’re going to face both internally and externally?

And how do we shape our strategy based on that? And I'd say just on the cyber Intel and Red team front, I have a, a weekly talk with my Cyber Intel team. As you know, the threat landscape is constantly changing, right? So, to stay fresh on what's happening in the threat landscape, I'm talking with my threat team once a week and getting a CSO level. What are the threats doing? What are the attacks there? Conducting? Who's falling victim, and how can we stay ahead of those? And that direct line from between me and my Cyber Intel team is actually shaping some of the decisions that I'm making on a week over week basis, because we have to be as agile as the threats.

John R: Makes perfect sense. Clearly, your background as an Army Intel Officer comes in handy. Understand what the bad guys are doing. Understand your threat profile and risk profile to align resources against against the threat. Kelly, back to you. Same situation: Limited dollars.

You're, I believe, county, type system there. You know, always operating on thin margins, but a great again, Steve Purvis CEO leader, participates with us on our healthcare advisory council with the federal government. How are you prioritizing cyber investments?

Kelly S: Yeah, I think, you know, all of my colleagues really hit on all the areas. I got a little misty eyed with Adam where he was talking about the missed framework. We adopted that about eight years ago. So, I'm a huge proponent of that. I probably would amplify a couple of things: One is education, to both, you know, board level executives and clinical staff.

When I joined Valleywise Health, 11.5 years ago, again, coming from other industries, with all due respect to my clinical brothers and sisters, I would say getting a hospital is really a data processing facility that takes care of patients. And while that's a little bit tongue in cheek, I wanted to set a tone of I'm absolutely hands on, patient care critical. However, we're all doing it with systems and technology and data.

So, education is key. Board education is key. We've started to see some improvement in investment, but as a safety net hospital, I wish I had an Intel cyber team, Adam, so I'm going to leverage yours.

But a couple of things I would use for our colleagues on this call. 4 or 5 years ago when I would deal with partners in cyber insurance carriers. Those cyber insurance questionnaires were 4 to 5 pages. The last one we did was 49 pages. So, what's happening is the cyber insurance business, as we all know, how does insurance companies make money? They don't pay claims, so they're putting more of the bullies back on our organizations for those defenses.

And so again, I would leverage that for our hospitals, CIOs and CISOs to be able to say, look, even the industry is saying table states are to have these types of technologies, these types of systems, these types of staffs to be able to protect the environment.

So, I think is what we're saying is, it is changing the dynamic and are going to go back to the education, to the executives and to the board. And here's a, I think, a critical skill for all of us. We have to be able to translate technology threat to, you know, I used to call it junior high level. But it's got to be pretty simplified so people can understand the threat and the impacts so we can turn those folks into advocates for us.

John R: Totally agree. Kelly, thank you for bringing that point up. Not only is cyber leadership issue, it's a translation issue.

Sunil D: John can I can I just a quick comment that, I just want to you know, those are for you who are on the panel and those of you who are listening, you know, we talked about operating without digital capabilities, an analog three years back. You know, we were pretty low in our maturity cycle. But, those of you who are listening, you know, this was, again, with a strong partnership with John doing tabletop exercises with our every single business function, educating and doing and enabling more, you know, how to conduct these downtime procedures and how to operate without digital capabilities. I think we have come a long way in the last three years.

So if those of you who are really interested, I’m very grateful to John that he partnered with us and we partnered with hundreds of our senior leadership, and bringing them up what it means to operate when you are in an analog mode, even for newer breed of residents and doctors who are... who really don’t have any experience in operating in analog mode, versus the folks that were already fully trained and operate in digital mode.

So, I just wanted to share that partnership. Well, for John and his contribution to our system.

Kelly S: So do I have to jump in just quickly because, when we had the CrowdStrike issue. Sunil, just just to amplify that point, we're teaching institution as well. We had residents that had never written a paper prescription before, and so we've had to put that into now our downtime procedures, literally, how to write a paper prescription on a discharge of a patient because, a doc coming out of, residency now has never done that, so...

John R: Again, technology has really advanced healthcare, improved millions of patient outcomes, saved countless lives. But it also creates risk because of based on our dependency. Sunil, thank you for your kind, gracious words. We looked for your leadership as well, especially in everything that you're doing there at Atlantic Health System.

Amit, I'm going to go over to you. We're going to change gears here just a bit, sort of in the third-party risk area about external threats.

There's a lot of M&A activity within healthcare being driven by the economics, quite frankly, for organizations, hospitals and health systems to survive, there's often this merger and acquisition strategy. Amit, from your national perspective, I'm sure Accenture has been, instrumental in advising on some of these transactions. How how do M&A factor into a cybersecurity strategy? And how does a hospital health system ensure, in, from your perspective, a seamless and secure integrations of systems – some might be more secure than others– post M&A?

Amit G: Sure. And I think just just as a basic I think we've worked with a lot of partners in terms of M&A, especially going with them, doing a due diligence, understanding the policy compliance gaps and some of the other thing. But I think your question is more strategic about the integration. Right.

So, what we do is primarily working based on our comprehensive due due diligence and, risk mitigation and third party risk assessment. We worked in terms of detailed integration planning. And in some cases it's different based on different cases, right?

Based on the risk and the level of maturity of the organization, which is coming as part of it. Right. So basically, you decide the pace of integration and phased integration of technology based on that risk, right? Which can if you take some of the example are, if I can put some example are. There are organizations where we feel that they might not be rightly enabled to start with the integration to start with. And that's where we work with in terms of either putting in network segregation. We talked about how do we put a zero trust or how do we do it, identity, maybe keeping a separate identity or do a very limited integration.

So, I think it's case by case basis, John, it's based on the risk profiling from the third party risk assessment as well as integrating asset in the early stages of the due diligence as part of the mergers and acquisitions.

John R: Yeah, thank you for that. Amid again, cyber due diligence for the transaction as much as financial due diligence has to be because ultimately it's about risk. And if there are significant cyber risk associated with the transaction, it will impact the financial calculus of the transaction.

Let me go back to Adam on this large health system. Right. I think you guys have certainly been involved in M&A over the last few years. What about, from your perspective, another issue that probably keeps you up at night?

Adam Z: Yeah, it does. It keeps me up at night a little less than it used to. But as you mentioned, yeah, Providence has grown by M&A over the last several decades. I mean, throughout our history really Providence and Saint Joseph's health and Swedish and, with every transaction comes some level of risk. In fact, earlier this year, we had an incident on an M&A; one hospital that we had purchased in California, we had an incident that, impacted that hospital. And I just say as a general principle, you want to migrate, not integrate with any M&A that you do. And I mean, migrate applications out of the acquired entities ecosystem into yours after you conform them to your security practices, migrate the users out of their ecosystem into your ecosystem, doing smart change control to do things like make sure that their multi-factor authentication conforms to your multi-factor authentication standards, for example, and use one suite of cybersecurity solutions across your entire ecosystem, not multiple suites that you inherit through those M&A.

But taking a step back, I would say strategically, cybersecurity needs to be a part of all those processes. At Providence, we have cybersecurity checks and balances throughout the M&A process. And cybersecurity has a seat at the table to influence the terms of the deal as well. And I think done right you can get a good sense, you can't get a perfect sense, but you can get a good sense of where the organization that you're acquiring stands from a cyber maturity perspective.

During the initial set of conversations, you can get a good sense of, does that organization have a shadow IT problem or a legacy tech debt problem. And I'll admit, we all have tech debt problems and in healthcare because of the third-party relationships that we depend on. But you can get a good sense of if the organization

.

you're acquiring has a serious tech debt problem, that's going to require a lot of investment to remediate pretty early on, and again, build those cybersecurity terms. End of the deal, that technology terms end of the deal so that you're compensated, as a part of that deal to bring that in up to snuff when it comes to the tech debt that you're going to have to remediate, just as one example.

But again, migrate, don't integrate. Do not integrate the IT systems of the acquiring entity into your, into your, broader ecosystem because you're inheriting all of their IT risk into your operating environment when you do that. And that comes with a tremendous level of danger.

John R: Right. Great points. Migrate, don't integrate, assess a cost. What that risk cost is what the what does that mean of the transaction. And I know that during these M&A transactions, you're limited on to how much visibility you can have into the organization before the deal. So it's a little bit art, a little bit science, and you got to roll the dice a bit from what I understand in these transactions.

So let me go. Sunil, Atlantic Health has grown pretty significantly over the past few years, and I think you all understand the potential risks that comes, with these acquisitions very well.

Sunil D: Yeah, that's a great, discussion point and I think Adam covered it very eloquently. And again, the key part is that you are not doing this exercise due diligence post-merger. You have to do this pre-merger. That's the key part.

Secondly, you know, you have to understand the footprint because not everything can be migrated or integrated. Integrated cannot be but migrated also. So you have to prioritize what is your scope in terms of... in terms of putting people and identities and and systems into into our own systems. But there will be systems, there will be data centers that have to be left behind because mergers and acquisitions always happens in phases. You cannot right away, you know, shut down and and remove the technology from the acquired entity. So most important issue is again prioritizing, you know, if certain things are not very important, but they will still remain there either because of because they are so unique that you do not have as a acquiring entity equivalent to what the systems you you need to merge. Then you have to create a very strong, robust DMZ framework around that so that they are then they are secured. Second part and most important part is identity management and segmentation. That's a key part when you are doing this acquisitions, because God forbid if something happens and things happen, especially on the weak, weak technology footprint and vulnerabilities.

Last thing you want to see is that the risk and the vulnerability gets propagated into your environment. So at least you should be able to shut down and contain the blast within those systems and isolate those systems, wherever they are. So that's, I think, some of the key things. And, you know, again, prioritizing investments, there is always a competing need for where the dollars should be invested and

and where the resources should be allocated. So, you know, super, super hyper prioritization is that is the key.

John R: Thank you, Sunil. [INAUDIBLE] from MD Anderson. What what are your thoughts on mergers and acquisitions?

Less S: So luckily we have pretty much grown up organically. But I would continue with what Adam and Sunil have been saying, doing the due diligence and not, basically bringing all of their people into your systems as opposed to integrating their systems. It’s just really good, solid cyber advice.

John R: Thank you. Kelly, your thoughts?

Kelly S: Yeah, I would concur. I think you've got to absolutely have technology, you know CIO, CSO at the table on any M&A activity, in past lives that was fairly common. I think now in healthcare, it's a little bit different. Our health system really doesn't grow that way; again, as you said, it’s a safety net. But, I think a couple of things; both, you know, having those, defined processes for M&A. And I really appreciated Adam's commentary there. The shadow IT I think we touched on that that is incredibly challenging.
But again, good process of new technology introduction I think will thwart a lot of that capability. So absolutely, I think it's all about integrating technology into the business. That's really the key.
And, you know, one of the areas, John, that that I think is an ongoing challenge in our industry is also where does the CIO and the and the CSO sit in the organization? Because I use that as an incredible bellwether as to the importance of the function is to the executive visibility and what table are you at. So, I'm always sensitive about that as well.

John R: Great point. When I'm trying to get a very quick pulse check on the cybersecurity posture of an organization. That's the first question I ask who does the CSO report to and how far is it that position from the CEO.
If in fact, you know, most likely most of us have the CSO report to the CIO and most of the time that works great. You have a technology leader reporting to another technology leader. If the CIO prioritizes cyber, if they don't, then that's probably not the best place. And it's risk legal in other other areas. Perhaps it's better suited for that function.

Kelly S: I agree 100%.

John R: Last, question here, and I think I'm monitoring the chat here on this great discussion we're having. I think we’ve actually answered most of the questions that have come in. Last question here in the remaining few minutes will we’ll get through this kind of a speed response here.
How are your organizations managing cyber resilience? We’ve talked a lot about resilience and recovery here. Managing cyber resilience

and ability to recover quickly from cyber-attacks, but also especially from third party cloud providers.
You might not be attacked directly, but our third-party cloud providers attacked and suddenly, because of years of thought to move to the cloud is better. We're suddenly left without an on prem backup solution. Go to you real quick, let's start off the top. What are you seeing across the United States from the Accenture position?

Amit G: I think one of the key thing, which we have to start thinking about is the realization in terms of that you can't stop the attack, right?. Which means there’s a lot of focus in terms of incident response plan, focus on operational resilience, making sure that there a clear alignment in terms of having a regulator regulated similar simulation attack or even having the right level of data in terms of mapping between devices and business services, I think the more focus is now what we are seeing it is that are then protected more about resilience and recovery, including the operational recovery piece.

John R: Exactly. Adam, over to you. And then then back to Sunil, Less and Kelly. So, Adam, over to you.

Adam Z: Yeah. Just really quickly, I think what I'd say is, you know, as a healthcare system, we were, I would say, less impacted by the change healthcare incident than some other major healthcare systems across the country. And we were able to recover pretty quickly from the CrowdStrike event. But I tell you, we use those two incidents, those two events as great learning opportunities to bring together different elements of the business and talk about what does it mean to be a resilient business.

So, organizations like risk, legal, communications, operations, we're all having conversations now, Providence about what is a mature business resiliency program look like and how do we manage crises at the top level and really institute lessons learned from those two major events into the plans.

John R: Leverage the crisis, leverage the events. Sunil, I think we go over to you.

Sunil D: Sure. And the way we see resilience is, you know, in different lenses. Resilience is all about how do you come back and how quickly you can come back.
So, there are three things that comes to my mind: Mean time to detect, mean time to respond, and mean time to recover. If we can shrink all these three things, you are able to recover fast.
Now take another three things, three sets: capacity, capability and preparedness. Capacity means do you have the resources, first of all, to go through this, crisis? Who would be responsible for for recovery? Second is capability. Even if you have resources, do you have the right skill set with that capability capacity team to really act in the way so that

they are able to do the right things?

They are able to make the make the right decisions to recover fast. Even if you have capacity, even you have capability. If you do not have the third component that is preparedness, which I talked about, where you really help us. How do you operate in analog mode from digital?

So, you need to have this as a muscle memory, because even if you have capacity and capability, and if you have never done done the downtime procedures on operating in an analog mode, everybody will be in the chaos when when the events happen.

So, you need to be prepared to have these capabilities. And talking about sources cloud, my personal view is when the events happen, it will happen whether on the on premise or on the cloud. It's just which way we can contain the blast, which way we can recover fast, and some of the cloud providers, you know, but we have to give you credit where it belongs. They spent billions and billions of dollars and their posture is, you know much more stronger. They do a lot of things that as an individual entity and organization, you cannot spend that kind of money.

So, they have smart capabilities. It's just that by moving right workloads to the right cloud and having the right oversight of their security posture versus our security posture, as you mentioned correctly, together you are in a much better position to take advantage of the cloud. You went to recover fast.

John R: That's great. Thank you. Let's I'm going to go to you real quick and we're gonna wrap up really quickly.

Less S: Yeah. So, we do have a major incident management process that basically connects us anytime we've got a anything that goes down in folks as well as our incident command structure.

So literally moving between a failure over to a downtime procedures is almost seamless because we get everybody on a call, anytime that we have even the smallest system go down.

So, when we have a third party, we can quickly and basically communicate that to operations as well as to our incident command folks to basically make sure that we can still continue to run the hospital.

John R: Thank you, Less. Merging of incident response with emergency management, business continuity, clinical continuity, disaster recovery. We've got to merge all these plans. Kelly. Yeah, there was a question came up. I just want to clarify really quickly on the pacemaker. So, I just want to emphasize to folks, we do not see this as a wholesale issue in terms of attacks on pacemakers. We're not aware of anything specific. There's been a lot of talk about it. What we do see is all the technology that, connects the telemetry and so forth goes down during the ransomware attacks.

We want folks to rest assured we have not seen direct attacks on pacemakers.

Kelly S: There's an interface between a pacemaker and the programmer. So, there is an air gap a little bit between those two, so.

John R: I just want to clear that flag for that. And before I turn it back over to Jennifer, I just wanted to thank you all. What an outstanding conversation.
Thank you for providing us the benefit of your experience. And thanks to all that tuned in, I want to thank all our network defenders, our frontline healthcare heroes for everything you do every day to defend networks, care for patients and serve your communities. Jennifer, back to you.

Presenter: In the next few days, all attendees will receive an email that will include a link to the Archives Leadership Scan session. You'll also receive a post-event survey that will allow you to earn a CHE credit.
Thank you all for joining us, and thanks especially to our panelists for their valuable insights. And finally, we're so grateful to our sponsor, Accenture for making this session possible. This concludes today's program. Have a wonderful afternoon.

John R: Thank you all.