FDD Media Call: Healthcare Cybersecurity Needs a Check Up

June 3, 2024
Featuring Michael Sugden and Annie Fixler
Moderated by Joe Dougherty

DOUGHERTY: Greetings. We will begin the call in about 30 seconds.

Good afternoon, many thanks for joining us for today's call. My name is Joe Dougherty, senior director of communications here at the Foundation for Defense of Democracies. We're a nonpartisan research institute focusing on national security and foreign policy, and we're based in Washington DC. We're grateful that you've taken the time to join us today as we address what some may think is not a national security threat, but in fact really is a significant national security threat, namely how cyber criminals are targeting and exploiting US hospitals and hospital systems, in particular rural hospitals. Joining us on today's call are the co-authors of the new FDD report, “Healthcare Cybersecurity Needs a Checkup,” which each of you has received. Please let me know if you need me to resend it. I'm happy to do so.

With us today is Michael Sugden. He's a research analyst and editorial associate at FDD’s Center on Cyber and Technology Innovation, where he focuses on issues related to nation state cyber threats, critical infrastructure protection and US cybersecurity policy. Annie Fixler is director of FDD’s Center on Cyber and Technology Innovation. She works on issues related to national security implications of cyberattacks on economics targets, on adversarial strategies and capabilities, and US cyber resilience. Both Michael and Annie contribute to the CSC 2.0 project. For those who are not familiar, CSC 2.0 preserves the legacy and continues the work of the congressionally mandated Cyberspace Solarium Commission. That commission issued more than 80 recommendations to reform US government structures and organization, promote national resilience, reshape the cyber ecosystem, operationalize public private collaboration, and preserve and employ military instruments of national power. At the commission's planned sunset, the commissioners launched the CSC 2.0 project to support continued efforts to implement outstanding CSC recommendations, provide annual assessments of the implementation of CSC recommendations and conduct research and analysis on several outstanding cybersecurity issues identified during the commission's tenure.

Protecting the nation's hospital systems from cyberattacks is part of this research. That's a lot and Annie may add to that in a little bit. But first, some quick housekeeping. First, today's conversation is on the record. We will share the transcript and a link to the recording from today's call within about 24 hours, hopefully less. Today's run of show is as follows. First, we'll hear from Annie with a brief introduction, followed by Michael who will walk us through the research findings. Annie and Michael might have some back and forth in that conversation. And then we'll open it up to questions and answers. You can submit your questions via the chat feature or you may use the raise hand feature in which case we'll let you know when you've been unmuted and you can ask your questions. Okay, that's a lot of housekeeping. Let's get underway. Over to you Annie. Thank you.

FIXLER: Thanks, Joe and thanks everyone for joining us today. So yes, as Joe mentioned this paper is part of CSC 2.0, we at the Center on Cyber and Technology Innovation at FDD, work with the former commissioners and other stakeholders to continue the work of the Cyberspace Solarium Commission. A lot of the work around CSC 2.0 is focused on public-private collaboration and particularly around critical infrastructure security. Our work on critical infrastructure security specifically focuses on sort of two batches of critical infrastructure. As you all know, there are 16 sectors of critical infrastructure, but we at CSC 2.0 and at CCTI more generally think about critical infrastructure particularly in two baskets. Critical infrastructure that is important and vital to the projection of US power abroad, the mobilization of US military forces and the like. And then secondly, and perhaps even more importantly, lifeline critical infrastructure. Critical infrastructures that are essential to daily American, life that impact American citizens every day. Our work in that lifeline sector effort has focused around energy and water, and most recently in healthcare.

Healthcare has really been one of those sectors particularly hurt by ransomware attacks. I think the trend line is moving in the wrong direction on ransomware attacks on healthcare sector. And so we wanted to understand what CSC 2.0 could contribute to that conversation, again as we look through the lens of public private collaboration. But we weren't content to just look at the healthcare and public health sector as a whole and to just add to the conversation. We're always, at FDD, looking for a piece of the conversation that's missing. And we felt as we were surveying the landscape of research that was being done on the sector, there was a real gap in understanding of the impact on rural hospitals and critical access hospitals that cyber threats are imposing.

And this is an important part of the conversation that we wanted to make sure we brought to light. So the report that you all have covers the sector as a whole, but with a particular lens of that rural healthcare sector cybersecurity. So that's sort of the thinking behind why we conducted this report and what we hope this report will add to the conversation. I'm going to turn it back over to Mike to walk you through some of the key findings of the report. Mike, over to you.

SUGDEN: Right. Thanks, Annie. So yeah, I'll start off by going over some of the major findings that we came across while researching this report. As you all know, the healthcare and public health sector has gotten a lot of attention recently for its cyberattacks and deservedly so. In fact, the sector is targeted by ransomware attacks more than any other sector according to a 2022 FBI report. And this is likely because cyber criminals are motivated to choose easily exploitable victims who are most motivated to pay. And many healthcare providers fit really snugly into this category because many providers often do not have robust cybersecurity teams to defend against attacks. And a ransomware attack on a hospital can really become a matter of life or death. So technology has become an essential force multiplier in the healthcare industry, allowing fewer doctors, nurses, and administrative staff to accomplish more work than they could have just decades ago.

And this evolution's been great, but ransomware attacks can knock out these key electronic functions in hospitals that force the staff to be stretched very thin. This slows down the entire medical care process and can lead to various complications. If electronic records become inaccessible, caregivers may not know previous diagnostic information, medication that patients use - and many patients may not know the medications themselves off the top of their heads, - or important test results, which just slows down the entire process and can also lead to complications in a worst-case scenario. So the biggest threat from ransomware though, we believe is the increase in time it takes for patients to receive emergency care. For some medical complications such as cardiac arrest, mere minutes can be the difference between life and death. And if a facility is affected by ransomware and cannot treat time sensitive conditions like this, patients may need to be re-routed to alternative facilities.

That additional time can be catastrophic. So while a delay in patient care is an issue everywhere, patients at rural hospitals face by far the biggest threat. Most rural hospitals fall into the category of critical access hospitals, like Annie mentioned, which are by definition at least 35 miles from any other hospital. There's other things too, such as they have to have 25 or fewer beds, but the distance is the thing that we're focusing on the most. And that's because if one of these facilities suffers a ransomware attack and can no longer say, treat cardiac arrest or pulmonary issues, these patients now may need to be rerouted to facilities an hour or further away. And the lack of alternatives for care is a unique challenge that is faced only really by rural hospitals and is the reason why we focused on rural hospitals in this report. There are many urban hospitals that may face similar financial issues to rural hospitals, but in DC alone, there's six general hospitals and then there's a bunch in Maryland, Virginia, right? like the alternatives for care exist.

So yeah, not only is this a threat to human life, but hospitals can also suffer massive economic damage. Rural hospitals already struggle financially, with studies showing that about 50% of rural hospitals operate at a loss every year. And a ransomware attack can cost millions in lost revenue and remediation cost. Not even including if they choose to pay the ransom. And this could be catastrophic and really the last leg for a hospital. And sadly, this really is not a hypothetical.

St. Margaret's Health in Illinois directly attributed their closure to costs associated with a ransomware attack. So they had to shut down because they couldn't afford to keep up afterwards. And yeah, hospitals exist to save patient lives, but they cannot achieve this if they do not have proper cybersecurity measures in place. Cybersecurity can no longer be treated as a second or third order concern. The sector and its government partners are both moving in the right direction, but at a pace that does not keep up with cyber criminals' ambitions, which is a huge issue. High profile attacks like Change and Ascension, that happened just in the past few months, are highlighting the need for action, and hopefully we'll see some good come out of these awful attacks. And Annie, I'll kick it back over to you for some recommendations.

FIXLER: Yeah. I want to jump in on the Change Healthcare comment that Mike just made. As we were putting the research to bed for this report, Change Healthcare happened. And we all saw in real time the interconnectedness of the healthcare and public health sector and the fragility, frankly, of some of the components of the sector when it comes to resilience against a cyber attack.

We at FDD hosted an event earlier this spring, at which Director Easterly, Cybersecurity and Infrastructure Security Director Jen Easterly, she was on FDD's stage and she admitted in front of the crowd that, while UnitedHealthcare was on CISA's list of what are known as systemically important entities, entities that have an outsized impact because of their size, their position, the way they cross sectors, and that CISA understood the impact of UnitedHealthcare. They were not aware of the impact that an attack might have on Change Healthcare.

That was a big oversight, a misunderstanding of the sector that CISA has now wised up to, and HHS understands. We all, the public, understand that much more than we did before. But we can't let this moment happen again. We collectively missed a systemically important entity. We can't miss others. So we need to do a much better job of assessing, what are systemically important entities? And so our report calls out that particular recommendation.

And I think you're seeing the administration move in the right direction on systemically important entities with the call-out in the National Security Memorandum 22, which has a specific mention of the need for identification of systemically important entities. So I wanted to pull that recommendation in particular, but Mike is going to go over a couple more of the recommendations in the report itself. So back over to you, Mike.

SUGDEN: All right, thank you. Yeah, like Annie mentioned, I'll go through just a few more that I really want to drive home. There are about 13, so I'm not going to list every single one, and you can get at it for your reading pleasure. But yeah, I think one of the most important recommendations that we have is the need to fund HHS SRMA capabilities. The Department of Health and Human Services is the sector risk management agency assigned to the healthcare and public health sector, but we've found that they have a really small staff that is fully dedicated to critical infrastructure protection within ASPR, the Administration for Strategic Preparedness and Response.

And in the past two years, their two budget requests have requested five full-time or equivalent staff, which would be a massive increase over what they have now. But we still think this is just too small. The healthcare and public health sector represents a whopping 17% of US GDP, and our SRMA funding needs to be reflective of that. We cannot have such a critical sector not only that is a huge part of our economy but is directly responsible for saving Americans' lives have just a few people dedicated to their protection.

We also think that the HHS should work with industry to prioritize life-saving services and securing those life-saving services. An issue that we've found many hospitals suffer from is hyper-connectivity. They will have many IT and OT, information technology and operational technology, across their facilities. Hundreds of different devices all connected together. And this isn't always the case but it oftentimes can be. And this presents many ways that hackers can get malware introduced to the system that can then spread pretty much anywhere if segmentation is not correct. So we believe that these critical services such as dealing with cardiac arrest, pulmonary issues, brain aneurysms, those types of medical complications, the equipment that can deal with those should be segmented off. So if you're at a rural hospital and there is a ransomware attack, we know that we can still secure cardiac arrest victims.

So then another one that we really think we should drive home is the sector-specific goals that the HHS released this year. There are 20 sector-specific goals that were reduced from the 38 that CISA put out as cross sector-specific goals. And we believe that these should be iterative and they should be continuously updated as hospitals begin to adopt them and provide feedback. We don't think this should just be a, "Here's 20 and this is it forever."

We also believe that a really great part of these CPGs, that they're divided into Essential, and I'm blanking on the second word. Enhanced CPGs. And the Essential are the most basic that should be funded immediately. And HHS is providing an incentives program that will provide $800 million to small hospitals that struggle to afford these cybersecurity goals. And the goal is that the fiscal year 2025 budget is going to request this money. However, this money will not go out to get these CPGs into these hospitals until about 2027.

So we fully believe that this needs to be moved up. 2027 is simply too far out. We know that there is all these issues happening right now. Hospitals are closing, patients are potentially dying, and this is something that needs to be solved immediately. Yeah. So those are some main takeaways. Joe, back over to you.

DOUGHERTY: Thank you, Michael. Thank you, Annie. Very much appreciated. We are now prepared to open it up to the Q&A portion of our call. We do welcome and encourage your questions. A reminder that you can ask your question by either typing it into the chat box or by utilizing the raise hand feature. As moderator, I will ask the first question. Annie and Michael, you both mentioned, both briefly addressed the attack on Change Healthcare. Can you elaborate a bit more on the findings related to Change Healthcare?

FIXLER: Sure. I'll get it started and then Mike can continue. So for those who have not followed that as closely, Change Healthcare is a payment processing company. They do a number of functions, but they're a large intermediary between hospitals and insurance companies and pharmacies to transfer the information, the financial information, verification of pre-authorizations, verification of insurance coverage.

So when hospitals and pharmacies can't do that, that means patients need to delay care or patients need to delay pickup of prescriptions or patients to pay out of pocket for their prescriptions. And this persisted for many weeks, including on our military bases around the country. And this is, I think, why that attack was particularly devastating, I would say. Perhaps that's too strong a word, but it feels like the direct impact on patients was significant, and it was nationwide, which is new, I think, from what we have seen in other ransomware attacks and other attacks on hospital systems, which have tended to be either a localized attack or even just an attack within one particular hospital system.

And this was significant because it was nationwide, because those effects rolled onto additional providers, had impacts against small providers, your local doctor's office. This isn't just hospital systems, these are individual healthcare providers. So that is why we need to understand the intricacies, the interconnectivity of the sector much to understand if there are other places that have that nationwide effect so that those systems can be protected. What does the US government need to do to make sure those companies are improving their cybersecurity? Segmenting, backup systems, resilience systems. And there's likely lots of carrots and sticks involved.

There are some incentive programs, there are some penalties. And I think our paper touches on some of both of those things but I think Change is a dramatic case study of why this is important. Mike, I don't know if you have more to add to that comment.

SUGDEN: Yeah. Just carrying off on that final point that you were making is that I think the fallout of Change Healthcare was so significant that really, now this isn't just one hospital or a couple hospitals that are suffering. Now it's really showing that this is such a national issue. And if you watch the hearings that the CEO of UnitedHeath Group, the parent company of Change Healthcare, the Senators, the Congressmen, in the two separate hearings, many of them had personal stories of their constituents who would write in or call them and say, "Hey, this is seriously affecting everyone's lives," and their lives in particular.

And there's been a lot of reaction from HHS and from Congress, too. Hopefully we will see that. Again, hopefully there will be a silver lining to how bad of an event this was, that maybe we will continue to have greater push-through and greater focus on cybersecurity. And again, this can't just go away and people can't just be like, "Oh yeah, cybersecurity. Who knows? It's fine." But I think this, it's really going to bring much more focus.

DOUGHERTY: Christian Vasquez of CyberScoop submits the following question: it does seem like a lot of what can be done relies on Congress to approve additional funds. If Congress cannot, will not, won't, et cetera approve more funding, how much can realistically get done, particularly when it comes to rural hospitals?

SUGDEN: I can take a first stab at that. It's going to be tough. One of the biggest issues with rural hospitals is they just cannot afford to... Or they cannot or do not dedicate a lot of money towards cybersecurity. And it's hard to blame them because a lot of, like I mentioned, over half of them are operating in the red. It's not like they're bringing in tons of revenue. So these CPGs, these sector specific goals that HHS has put out, it would be great if that incentive program is funded by Congress because it could supply some of that money and subsidize the cybersecurity gains. But if Congress isn't behind it, I'm not super optimistic.

FIXLER: Yeah. I will admit I'm not optimistic either. This does come down to money in a lot of the case. I mean, it is about better funding, HHS as a sector risk management agency, providing funds to hospitals who can't otherwise afford to increase their cybersecurity. There are some things around the margins, I think, that we can get done without additional funding. And part of that really comes to, when it comes to rural hospitals, of including them in the conversation.

As you all know, there are large industry led organizations that are effectively working with the US government to understand the threat and to propose and iterate on policy recommendations. Our concern, however, is that rural hospitals may or may not be part of that conversation in the way that they need to be. And so, are the expectations for what hospitals can do set at the right level?

So maybe it's reasonable for certain minimum cybersecurity requirements to be unfunded at large hospitals, but at small hospitals or rural hospitals and critical access hospitals, maybe it's not realistic to expect them to even meet a minimum cybersecurity requirement if they don't have funding for it, if they don't receive outside funding. So maybe that funding is from the government, maybe it's from philanthropies.

Maybe it is better connecting of those rural hospitals with free cybersecurity training tools. There are a lot of free programs available, but we can't expect rural hospitals to know about them, to be able to utilize them without some sort of support. So I think, again, there's some things we can do without Congress, but a lot of this does come down to funding.

DOUGHERTY: It sounds like there's a role though for industry as well in this. Is that accurate?

FIXLER: Yeah, absolutely. I mean, there are existing industry organizations. There's the Health-ISAC, the Information Sharing and Analysis Center. Many of the critical infrastructure sectors have one. The Health-ISAC is an active ISAC. It has a strong membership. Some ISACs are free, some ISACs are not free for members. The Health-ISAC is not free, although they prorate their membership. And so large hospitals pay more, small hospitals pay less, but they can all receive the same benefits of information analysis, sharing of what other folks are seeing, which can help hospitals protect themselves or other healthcare providers. It's not exclusive to hospitals.

There may be a lot more that industry can do in that kind of space to make sure that rural healthcare facilities are part of that conversation and receiving the information they need so they make better choices and invest even those limited cybersecurity dollars in the most effective way.

SUGDEN: Piggybacking on that, even though, yes, these massive cybersecurity overhauls are going to be difficult without funding, some things such as cyber hygiene training can absolutely be achievable. For example, there's the statistic that about 91% of cyberattacks happen through phishing emails. So if you just don't know that this is a suspicious link because you haven't had the awareness of it, that could be it. That could be the ransomware attack. But there's a lot of free and a lot of really inexpensive tools to teach cyber hygiene.

And of course there is the outreach program that Annie mentioned that needs to happen. A lot of these hospitals, I think we talked to someone who said that a lot of these hospitals, it'll be a nurse, who is also their head of cybersecurity in a dual hatted position. And it's just you can't be dedicating... I mean, the nurses are already so strained doing their nurse jobs that a lot of times cybersecurity is hard to follow up on that. So outreach is definitely going to still be important. And the industry can do it in the meantime, obviously we still do want congressional help.

DOUGHERTY: We do have another question in from Jonathan Greig. What does the next year look like in terms of cyber attacks on rural hospitals? Are we due for more ascension-like incidents? And he follows up, where does FDD land on the issue of who is at fault? There's a question for you both. Hospitals say it's technology providers like Change Healthcare and technology providers say it's mismanagement. I think Michael, you mentioned for example, no two factor, et cetera by hospital IT teams. Are both equally at fault for most incidents that you examined? Over to you.

SUGDEN: I can tackle the first part first. I think that's definitely the easier one. I think that attacks in rural hospitals are not going to get better until the support happens. You look at the CPGs and the funding that the administration has asked for, this money will not reach hospitals until fiscal year 2027. So there's really no reason to assume that rural hospital attacks are just going to magically get better in the next 12 months.

As far as the second one, that is a really tough question. You could say that there's a lot of people at fault, and that wasn't an attack on the hospitals themselves. And something like that you can absolutely blame Change for. At the congressional hearing, they revealed that it was an issue of multifactor authentication, and that's one of the easiest cybersecurity measures to produce. And United Health Group is either the 10th or the 11th biggest company in the United States by revenue. As far as other things, if it's just a standard localized ransomware attack, then it's harder to blame... It's really on a case by case basis. And maybe Annie can-

FIXLER: Yeah, I'll jump in a little on that.

SUGDEN: ... clear that up a little bit. Sorry, I'm rambling.

FIXLER: So in the case of Change Healthcare, I think you can blame a company of that size for failing to implement basic cybersecurity practices. This, as Mike said, this was the failure to implement multifactor authentication on an externally facing portal that according to their policies, they should have had multi authentication on, but they didn't. They are a multibillion dollar company. They should have the teams and the staff in place to know better.

It's hard to blame rural hospitals when you've got a nurse in charge of cybersecurity. That is asking too much of a small team. I think we would argue that those with the resources to implement cybersecurity measures should do so. Technology providers need to make technology that is secure by default and secure by design. You've heard those terms from CISA. That is about making sure that the technology can most easily be implemented with cybersecurity built in. So rather than expecting a poorly resourced IT team to understand how to configure a system, if you can make the product already have those built in. Or, things like when they install a new product, if there's a password, make them change the password by default. They can't keep a default password on because the system won't let it when you install it.

So it's things like that where technology providers, software providers, equipment providers, can bear the burden of the cybersecurity that will alleviate some of the strain on smaller entities that don't have the resources, don't have the expertise. So I hope that's what it gets to the point that you're asking about.

DOUGHERTY: How about state and local government, a role there?

FIXLER: Sure. I mean hospitals, some are private, some are public, some are municipal. There's a lot of different ways that hospital systems are set up. Local governments, state governments also can set up grant programs. They may have less flexibility than the federal government to create large programs, but that doesn't mean that they can't do targeted programs, specifically focusing some of their most needed hospitals. And they know their systems better than the federal government does, so they may know where to focus resources. So there's absolutely a role for state and local governments.

DOUGHERTY: Very good. That does end the question so far. We still have another few minutes if you want to submit a question. I think one just popped in. Yep. This from Megan Gates. Your report and research are focused on the United States. Have you done any research on how rural hospitals and other countries are addressing cybersecurity challenges with limited resources?

FIXLER: I'll jump in first. I don't know, Mike, if you have additional information. We have focused on the US healthcare system, in part because again, CSC 2.0 has that focus on public private collaboration, which is structured differently in the United States than other countries because of the way we define critical infrastructure, because of how critical infrastructure is designated in the United States how our sector risk management agencies are set up.

So we were specifically focused in that space. A couple years ago The Cyber Peace Institute, I believe that's their name, did a really interesting study on healthcare cybersecurity more globally. So I think I would point you to their recommendations and their research on that. But we sort of Primarily focused on the United States. But Mike, I don't know if you have additional thoughts to add.

SUGDEN: No, you said that beautifully.

DOUGHERTY: Very good. I think we'll take this opportunity to wrap up the call. Before I ask Michael and Annie to put together some final thoughts, I do want to thank each of you for participating in the call today, for dialing in. Thank you for reviewing the report that the two authors compiled. Both are available for interviews. If you want to have a one on one conversation, happy to schedule that. You can reach us at press@fdd.org to ask any questions. And did I see that a question popped up? Sorry about that. We're working on the fly. Yes. Actually, we do have time for this. We'll ask Christian's follow up. Thank you, Christian. Appreciate that. Curious how you all are thinking around the difference between policy resource discussions, around hospitals versus medical devices. Are there any connections here or are these separate conversations?

FIXLER: I'll jump in first and then Mike jump in after. So generally, I would say separate, but complementary and with some overlap. The conversations around medical device cybersecurity, I would say is a real bright spot in the sector. We didn't focus as much on it in this particular paper, but we've been seeing some really positive movement from FDA, when it comes to cybersecurity of medical devices. The FDA has been forward leaning on particularly requirements for new medical devices. I think there are challenges when it comes to legacy devices because a lot of where they have the ability to implement new standards, new requirements, is on new devices coming to market. But the FDA has been looking at new cybersecurity standards, the use of software bills of materials for medical devices. So you're seeing some real positive movement there. That will have effects on hospital systems because hospital systems use medical devices. But it is generally a separate conversation from the broader, particularly hospital networks, that I think we really focused on in this report. Mike, you want to add?

SUGDEN: Once again, honestly, I can't have said it better myself.

FIXLER: Great. And I will just say, since we brought up the topic, we've been looking at the question on software bill of materials for medical devices. Our colleague, George Shea, at the Transformative Cyber Innovation Lab, another component of the work we do, has been doing a lot of work on software bills of materials. And there's some really interesting work being done by the Health-ISAC, when it comes to the use of SBOMs. So again, really positive movement in that space. It's not all doom and gloom in the sector, but there are still some really significant outstanding issues that we think need to be addressed.

DOUGHERTY: Come to FDD for the silver lining. That is for sure. Annie, what's up next on the critical infrastructure research that you and the team are working on?

FIXLER: Sure. So as I mentioned at the top of this, we sort of think about critical infrastructure in the two baskets, what we call military mobility critical infrastructure and lifeline critical infrastructure. So we have next iterations coming through in each of those. Next up will likely be a report on aviation cybersecurity. This falls into our military mobility section. We're concerned about the impact of cybersecurity failures by the aviation sector and what it may do for America's ability to mobilize forces, were are we to need to mobilize in support of an ally or partner, let's say in the Indo-Pacific. That research is ongoing, but some really interesting findings I think when it comes to where the aviation sub-sector is really impacting and interacting with US military. That's next up when it comes to military mobility. Over on the lifeline critical infrastructure sectors, the two, I think that really deserve a lot of attention, that we're going to try to tackle next, food and agriculture. I don't think a lot of Americans understand that food involves cybersecurity. So we want to try to understand the ways that adversaries are impacting America's food supply and what it means for national security.

And then education. As we look, even as summer is just beginning, already starting to look towards the fall again and the start of the school year. And we saw in past years that cyber criminals know the school schedule just as well as we do. And August has seen a lot of cyberattacks against American school systems, and that is a problem and likely to get worse. So, that is where we can look ahead, where our research is going.

DOUGHERTY: And of course, we promise to keep each of you updated on that research as it becomes available. Michael, Annie, before we go, any final thought or two?

FIXLER: Sure. Let me jump in and just say, we have been, I would say pessimistic through most of this call, and we have a lot of concerns about the sector, but I think we are seeing the right movement in the right direction from the administration, when it comes to public-private collaboration on cybersecurity for the healthcare and public health sector. As we mentioned earlier, it really comes down to funding a lot of this. So we've got to, not just sort of talk the talk, but also put our money where our mouth is on this issue. So that's where we hope to see much more movement going forward. Mike, one last thought.

SUGDEN: Taking a step back to that pessimism. Like I mentioned earlier, many healthcare providers have treated cybersecurity as a second or third order concern, and that mindset is really proving disastrous. Cyber criminals show no sign of stopping the onslaught of ransomware attacks, and that is creating complications in patient treatment, that have ultimately resulted in people's deaths. And that is an unacceptable risk that we have, and we need the action, the funding, from government and industry to solve that. And that's it. Thank you.

DOUGHERTY: Thank you, Michael. Thank you Annie. Thank you for all the journalists on today's call. In closing, a reminder that FDD is a nonpartisan research institute, focused on national security and foreign policy. We closely monitor our press email that's at press@fdd.org. Please don't hesitate to email us any queries that you have, and we'll be glad to connect you with these and other experts. On behalf of Michael, on behalf of Annie, I'm Joe Dougherty, this does conclude today's call. Thank you.