Transcript Episode 19 Part II Michael Harvey

Ron Kruzeniski:

I'd like to welcome you to part two of my interview and discussion with Michael Harvey. Michael is the Information and Privacy Commissioner in Newfoundland. In part one, we talked about his background prior to becoming a Commissioner, and he certainly had extensive background in the health sector. I believe his background equipped him well to deal with the breach in Newfoundland in Eastern Health. This podcast part two, we're going to discuss that breach, the report that the Commissioner's office issued and the recommendations made by the Commissioner's office.

So, Eastern Health, now in Saskatchewan, we've had two fairly significant breaches. One was eHealth, which is our IT health provider and one was SLGA, but I think Eastern Health now probably ranks as a significant breach, not only in Newfoundland but across Canada. And I wondered if we can just talk about the scope of that breach, just how significant was it?

Michael Harvey:

Sure. Before I do that, I should probably give a little bit of background on the structure of the health system in Newfoundland Labrador and because it turns out to be a really important part of this story. So actually, the breach was not of Eastern Health per se, but of the Newfoundland Labrador Centre for Health information. So, the health system as it was at the time of the breach, which was October of 2021. There's six organizations that we are interested in here. We had at that time there were four health authorities.

These were the one that you mentioned, Eastern Health, which is the health authority for really the eastern part of Newfoundland, which includes St. John's and Metro St. John's area and some of the rural eastern part of the province. So, that's about half of the whole population is that one regional health authority. The rest of the province is divided up into what we sometimes call our rural health authorities, which were Central Health, Western Health, which is most of the western part of the province. And then Labrador Grenfell Health, which is the Labrador and part of the northern peninsula of the island. Those were the four health authorities.

And then there was the Centre for Health Information. So, the Centre for Health Information was created around 2000, and it was at the beginning of its existence and for years after it existed to essentially develop the electronic health record. And so, it was involved in developing applications and try to spread the use of electronic medical records across a province, setting up a pharmacy network and other key databases for the health system. But then in around 2018, the decision was taken by the government to move to a shared services model for the health system.

So, beginning at around that time, the Centre for Health Information assumed responsibility for all of the information management and information technology for all the health authorities. So, previously they had run their own IT and IM, but this now started to be run by the Centre for Health Information. And that change management was ongoing during the cyber-attack. So, the whole system was in the midst of this transition and even still, so this is why at the time the respondents of the report were all of the four health authorities and the Centre for Health Information.

And the sixth organization here is the Department of Health and Community Services. Because the department has, and the minister in particular under the legislation that creates these organizations has directional authority over both of them, even though every health authority had its own board and the centre had its own board, the minister had authority in the legislature to direct any of those organizations. And turned out during the cyber-attack, as is detailed in the report to exercise and coordinate the response. So, all of these players had a piece of the pie.

It should also be noted two other things that in June 2021, not long before the attack, the government announced that the Centre for Health Information was going to be folded into the department. It didn't really say how that was going to happen and this hadn't actually been implemented, but it made that policy decision. And so, that didn't end up really playing material part in the report, but it definitely speaks to the fluidity of the organizational flux that is occurring. And then after this has all happened, the government has made the decision and has now implemented the decision to collapse all five of those other organizations into one Provincial Health Authority.

So now, as of April 1st, there is no more Centre for Health Information per se, it is all one organization called the Provincial Health Authority. This organizational flux that is occurring and this complex change management that was ongoing is a relevant contextual factor for the investigation because it did create complications for accountability and cause confusion during the notification period. So, it caused problems before the attack and also cause some problems afterwards. Which is not to say that governments should not change their organization, governments change their organizations all the time.

But I think it's important, certainly a key takeaway, and this isn't one of our findings, but I think it's a lesson, I think. That when governments engage in organizational change, they need to be aware of the risk that they're creating for things like cyber-attacks. You don't launch into a change management being aware that it consumes resources, it creates a stress on an organization, and it exposes it to risk, and this is one of these examples. I think none of that is to answer your question, Ron, and I'm not trying to be evasive. But so, you asked a relatively simple question and then I answered a different, more complicated question. I'd probably be a terrible lawyer.

So, I'll answer the simple question that you asked, actually it does have a simple answer and that is what's the scope of the breach? But I needed to answer the first question first. The scope of the breach is personal health information in the custody and control of all the health authorities were effective, but they were effective variously. Patients in Eastern Health, so remember that's half the population had their information breached going back 11 years. Patients in Central health over 15 years, patients of Labrador Grenfell over eight years.

So basically, it seems the attackers didn't go into the Western Health portion of this database, at this point they probably figured they didn't even need to bother. But there were Western patients affected as well because anyone in Western Health who had sent their blood tests into Eastern had personal health information breached. And so, all of these people would've had their medical care plan numbers breached and information about them and then some information about what they were being seen about. This is the information in the registration database. So, this is really valuable information.

So, that's all four RHAs going back a minimum of eight years. That's pretty much almost everyone who's come into contact with the RHAs. And then putting aside all that, all patients who had COVID-19 testing within and across the province. So, who didn't have a COVID test done over the course of last number of years before October of 2021? That's some personal health information. Then there was the employee data for including social insurance numbers for Eastern Health. You note that Eastern Health is the largest employer in the province.

So, Eastern Health and Central, and in this case, it went back to 1993. Living, dead, all of that information, all those social insurance numbers for all those peoples, going back all that far. There were actually social insurance numbers also breached for a certain number of people that were living in long-term care, which leaves one to wonder why are you collecting social insurance numbers for people in long-term care? A good answer was never provided for that, it certainly does tell us when we look at this level of data here, you have to ask questions about records and retention and over collection.

The short answer to your question is that what happened is the bad actors got into the system, they were able to move laterally about the health system with relative impunity for about two weeks. During

which time they were able to see almost anything. But we know that they exfiltrated and took about 200 gigabytes of data containing the personal health information and the personal information of I would say almost everybody in the province. So, that's a broad scope of a cyber-attack. No evidence was provided to us, and we understand that there is no evidence that any of this data has been further breached, let's say.

Sold on the dark web or used for any nefarious purpose, we don't have any evidence of that. That's a good news story, but it definitely was, this data was exfiltrated.

Ron Kruzeniski:

So, your office faced with a breach of that scope, did an investigation, and as we've talked about issued a report. What would you say were the significant findings in that report?

Michael Harvey:

I'm going to start with the good news claims, why there were actually lots of findings, but there were only a few recommendations. And that's because the first thing is that since the attack, the government and the Centre for Health information have responded to harden the system and implement what they've called and talked about publicly, Project Breakwater to harden the system and to prevent further cyber-attacks to the best that they can. And also, and this is another picture even to the extent that they are not prevented to mitigate how bad these attacks are if they do occur.

You can do a lot to prevent phishing, but in large part, sometimes you're still going to rely on someone not to click that link and human error does occur. And so, you need to have many layers of safeguards in place. They've done a good job and not just trying to prevent phishing attacks, but also putting in the appropriate and industry standard safeguards to harden the system further. We issued as part of our report a confidential annex. This is the first time we've ever done that an issue, a confidential annex because we wanted to talk to them a little bit on things about what had been their vulnerabilities and the things that they have done since to harden. But we couldn't talk about that publicly for risk of further exposing vulnerabilities.

So, this is the first time we've ever issued a confidential annex as part of a report. But I think the good news is that if they keep doing what they have planned to do, then they're on the right track. Not only have they introduced this Project Breakwater, but they have got a secondary analysis of that project. A secondary expert analysis that has given them advice on how to even improve what they're doing and they appear to be following that advice. So, that's a second level of good. So, we're quite pleased about that. For that reason, we only had those six recommendations.

On the other hand, the notification, the immediate response to the attack and the notification was pretty good. First of all, what they did was immediately reach out and get expert advice as best they could and including expert strategic and legal advice from the top experts in the country in this area. And even though I would say that our investigators had some friction, which may be to be expected over the course of the investigation and some disagreements with them. But engaging those experts is the right thing to do. And these are both private consultants, legal firms, but also the Canadian Centre for Cyber Security and law enforcement.

All of that was done well and they followed their advice and that was very good. The notification, which is obviously the next step that we look at, was deemed to be pretty good and reasonable, but there were some gaps. A couple of them that we might highlight is there was confusion about whether the information was taken or not. And in fact, it took the government and the health authorities about a year and a half until they would admit that the attack was a ransom attack. And the government did in

March of this year issue its own report. So, this preceded our report in March of 2023. Only at that juncture did they admit that it was a ransom attack.

And to be honest, by this time it had gotten a little bit absurd. Everybody had assumed that it was a ransom attack. What else could it have been? But the government was not being clear about this, and I think their advice was not to do this for fear of further antagonizing the perpetrators. And that the perpetrators in early 2023, the FBI had announced that it had disrupted this group, which turns out to have been Hive and they had disrupted this group. And now that this group was disrupted, they felt that it was safe to come out and say that it was a ransom attack.

So, we note that first of all, Hive may have been disrupted, but there are cyber attackers all over the place, and it's not like Hive doesn't exist at all anymore, that all of these individuals are in jail or something, but they may have been disrupted. So, we query that, but we also look around elsewhere and find that public bodies in other jurisdictions are announcing and letting people know when there's a ransom attack much earlier and when the attack occurs, and this is material to the population. So, this is relevant, how they understand the risk that their personal identification is being used.

So, it is material for people to be able to assess the risk that they're under, knowing of what kind of bad actor is engaged and whether or not they've exfiltrated data, what they're threatening to do with it and those kind of things. So, these are things that we felt should have been part of the notification, and we think that it was not appropriate and not a proper notification, not compliant with legislation that they did not release this information until more than a year and a half later, until March of 2023.

There were other aspects of the notification that were complex and confusing. So, of all of those people, like I mentioned before, almost everyone in the province was affected, but some people were affected differently than others. Some people have the social insurance number taken, but not others. Some people had registration data including name, address, telephone number, and MCP number exfiltrated. Some other people had more detailed health information about them exfiltrated because Eastern Health had a network drive. I didn't mention this earlier, but Eastern Health and network drive taken, which had more detailed personal health information on it, those people got letters.

So, the employees and the people who were identified in the network drive, they got individual letters, but the letters came out in various waves because going through that network drive, we're talking about millions and millions of lines of code. The Eastern Health in this instance had to hire external consultants to do an assessment of all this, and it took a lot of time. Figuring out the employee data, that was also really complicated because like I said before, we're talking about employees going back to 1993. So, those people may have changed address or died or figuring out who needed to be notified of all of that, of those people. That was very confusing as well.

But I think the finding was they did their best and what they did was reasonable even though it was confusing. So, that's another set of findings that if I could summarize it's, notification was pretty good and complex with some flaws, but under a complex circumstances but there were key gaps that should have been done differently. Three other findings I want to point to. One is, as I said before, there was a complex accountability situation that was arising from the change management with the implementation of shared services.

And so, NLCHI received a highly fragmented and inadequate security situation that it should have been managing and trying to bring all those IT and IM systems together and really put them under a coherent and secure setting. The change management that it was undergoing at the time really made this a challenge to do. And it was challenging both the fragmented and inadequate situation that they were inheriting. And to be honest, their response to it was both inadequate. And anyone who's been involved in a complex change management knows those kinds of challenges are almost par for the course, but

nevertheless, not an acceptable par for the course because of the nature of the risk and the clear and present risk that the organization was aware of.

The other thing that made it particularly unfortunate, Eastern Health prior to shared services had started to prioritize cybersecurity, but basically had to put their tools down once NLCHI assumed their responsibility for IT and IM from them. So, that was an unfortunate consequence of the change management. So, that's another key finding. NLCHI, even during this, even though it was faced with a real challenge, the resources that had put towards it were ultimately deemed to be only three people. And our experts and the Canadian Centre for Cybersecurity all judge this as a really grossly inadequate amount of resources to put towards cybersecurity.

Another finding was that there were industry standards. The legislation says that custodians need to implement reasonable safeguards to keep the information safe. So, when we try to assess that question, we ask ourself, "Well, what is reasonable here?" Our act doesn't tell us what's reasonable, the act is technologically neutral. So, to determine what's reasonable, that can change over time. It can change based on the fact of the situation, right? So, we asked ourselves and our investigators asked ourselves and we asked our technical experts that we hired, "What are the industry standards?"

And we know that there are standards out there like NIST and ISO and so on. So, we know that there are standards, what is actually being used in the healthcare sector in Canada? What is the norm across the country? What we found was yes, there are these standards for cybersecurity, and yes, they are being used in the health system across the country. And yes, the Centre was aware of these standards and we found that they were not up to standards. These were standards, they were industry standards and the Centre was aware of them and they were not up to standards. So that is a key finding of this report.

Moreover, we found that the provincial government was warned about this. There was a briefing note that went in 2020 a year before the cyber-attack, a briefing note went in that said, "Listen, we've had this assessment done of the cybersecurity situation. Here are these risks." And the provincial government did not respond to it. The Centre for Health information has a statutory mandate and it has a responsibility to discharge the statutory mandate and it's guided by a board in doing that. But its resources come from the provincial government and in this instance, it warned the provincial government about this and the provincial government did not respond. So those really were the key findings of the report.

Ron Kruzeniski:

So, in canvassing those findings, you may have covered a bit of the next question, but I'll ask it anyway, and that is, in the report, it acknowledges that many steps have been taken, which resulted in the need for fewer recommendations. Were there a couple significant steps that all the entities took in terms of addressing the issue that resulted in your office not having to make a recommendation on the matter?

Michael Harvey:

Without getting into the details of what Project Breakwater is and the details of what it has implemented? There are some visible things that all of us can see every day because the provincial government has also implemented some of this stuff too. It is looked at its own information management systems and we have, let's say for example, you see much more use of two-factor authentication than was previous. There's warnings on all of our email and now I think almost every organization in Canada and maybe in other countries as well, you get a warning about an email that comes from an external source.

There's all of this general hardening has occurred, there's many different aspects of that. And then the other things that we see are more training that is being done and then more ongoing, always ongoing

review and oversight of the hardening that's being done. So, like I said, we've observed them do that and so far, we're pleased that they're doing it and some of our recommendations are focused on keep doing that. And I should have mentioned that the Provincial Health Authority now, which is a single organization that is responsible for responding to our report, has responded to it and indicated that it has accepted our recommendations.

They did mention, they don't necessarily agree with all of our findings, but they didn't actually specify which ones they didn't disagree with. So, I'm happy enough with that, but they did say that they accepted our recommendations and will be implementing those. I know that we can talk about those recommendations, but I'm pleased with where the health system seems to be heading and its response to this report.

Ron Kruzeniski:

So, in your office's report, they made six recommendations, and I guess you'd say all recommendations are important, but which ones do you see as quite significant that you're hopeful the whole health sector will follow?

Michael Harvey:

I won't go through every single one of them, but I will maybe start with the one that the health authority has decided to quibble with. Which I can understand their point, and that is do you have to notify the public if there has been a ransomware attack. They say, "Well, not necessarily and not necessarily right away." It will be the way that I would paraphrase their response is that they don't necessarily have to do it soon and that the assessment of when they need to do it has to be done in consideration of the fact circumstance.

I can understand this little bit of equivocation, and again, the law says that notification needs to be done when it's reasonable to do it. I understand this little caveat that they've thrown in there. But that is one that people need to know and deserve to know because it is material to them if the breach is related to a ransomware attack. Another one that we focus on here is records retention and destruction. Some of this information never should have been collected in the first place, like the social insurance numbers of people in long-term care. These are relatively minimal examples.

Although I will say Ron, and I'm not sure if you'd find the same thing. I know that when I was up in Toronto at the recent International Association of Privacy Professionals Conference and the commissioners who attended were on a panel and someone asked, "Which of the privacy principles do you think people have the hardest time with?" And I can't remember who answered the question, it might've been Commissioner Dufresne or maybe it was Commissioner Kosseim, but the answer was minimum use and collection of personal information.

I really see this the time with public bodies and health authorities that this idea, this principle that's entrenched in our legislation, but it's entrenched in all of our legislation. That public bodies and custodians should collect the minimum necessary personal information or personal health information to do whatever the legitimate thing that they're trying to do is. That is not commonly understood, even though it's not within my jurisdiction, I would say it's just as bad for private sector entities as well.

Organizations want to, some organizations want data mine, but even the ones that don't, I think they're inclination is let's get as much data as we can and let's get data that we don't even need because it might be useful in the future. So, this over collection phenomenon is a big one. So, I really hope that the Provincial Health Authority takes that to heart and spreads that throughout the organization because really when custodians and public bodies collect information, they really need to ask themselves, do I need to collect this?

And then once I have it, I need to keep it safe, and to put it me to keep it safe and make sure it's not misused, and breach is only one way in which it can be misused. So, I really hope that they take that one to heart. Another one that I was very pleased, and I've already talked about periodic assessments that be done and that this ongoing review and audit at reasonable interviews would be watching yourself. We are obviously not going anywhere, and we will always be a source of general oversight, but you've got to have the internal controls ongoing and put that in place.

In guiding this, we recommended the creation for this new Provincial Health Authority of a chief privacy officer position that should be at or reporting directly to the executive level. And we're not talking about a role that someone would do off the side of their desk, but a person who is specifically qualified and has experience in privacy with appropriately resourced staff and has responsibilities extending from the largest hospital to the smallest clinic, virtual care and will take a comprehensive approach to privacy.

And I had actually written the chief executive officer before the report even came out, when the Provincial Health Authority was being formed. I didn't want to wait until the report came out, and this was prior to my recusal from the investigation. I had a sense that this was going to be one of the recommendations and I wanted to write the CEO about this and recommended the chief privacy officer. I think even though here we're talking about security, cybersecurity privacy is not just cybersecurity either. I know that I'm preaching a converted here Ron or the converter as the case may be.

But privacy is multifaceted and complex, and so I wouldn't want a chief privacy officer to be the cybersecurity person. The chief privacy officer needs to look across the breadth of a range of different aspects and take a horizontal approach to a Provincial Health Authority and talk about privacy. Yes, as it relates to security, but also privacy as it relates to what's happening in virtual care and for that matter, non-virtual care. There's a whole number of different aspects of privacy that need to be considered, and the chief privacy officer therefore needs to be at that senior level able to exert authority across the multiple lines of business of this large and complex organization.

And so, I was pleased to see that even though in their response to the report that the health authority didn't explicitly say, "We're going to appoint a chief privacy officer," and it didn't say who it was going to be or anything like that, they did in agreeing to the recommendation I'm taking it that they accepted this recommendation. And so, I'm really looking forward to seeing who that is going to be and what their mandate and resources are going to be. And I think that there's models out there elsewhere in the country of chief privacy in health organizations, and I'm really looking forward to seeing how that unfolds here in this province.

Ron Kruzeniski:

So, you've covered so many things that I hope people in large organizations in the health sector pay attention to and read the report. But I think you and I and others, we don't say if a breach occurs, we talk about when a breach occurs in an organization. And from all of this, what advice, one or two things would you say to health organizations across the country or in fact any organization across the country in terms of what they should be doing or paying attention to in this whole privacy breach area or cyber breach area?

Michael Harvey:

I like that point that it's not if, but when. The other observation I've heard is there are two types of organizations, those that have suffered a cyber-attack and those that don't know they've suffered a cyber-attack. So, really the advice I got, and this isn't so much advice that I have because I think we've covered some of the lessons from our report. But some other advice that I've heard about a cyber-

attack preparedness that I want to pass on that I think is really valuable and that has resonated with me by understanding what's happened here.

The first thing I'd say is have a handbook. And so, there's one of these situations where you want, it's almost like a go bag or something behind glass where you run to it and pick it up and say, "Okay, we've suffered a cyber-attack, what do we do?" So, every large organization should have one of those. And I should point out the Centre for Health Information has one, but I think experts will say is, "Even if you have a handbook, the only way to be truly prepared for a cyber-attack is to have actually gone through one."

Because even if you are prepared, you can never really glean from the handbook what it is that is going to happen because you do enter a very surreal type of situation once it occurs. And a very fluid type of situation, particularly in the case of a ransomware attack where ransomware attacks are people that have been directly involved in them will tell you they're very bizarre. And that these organizations, the cyber criminals are very bizarre organizations. They're distributed in many instances all around the world.

Many of them are sometimes acting like they want to be legitimate businesses, even though they are very clearly engaged in a criminal organization. You'll talk to them and they will act as if they are legitimate businesses. It's like an Alice in Wonderland type of situation where you come upon the Mad Hatter and they're claiming to be running a perfectly respectable tea party when instead the whole enterprise, there's a criminal enterprise. There's this surreal aspect to how it all occurs, and so this is where the second piece of advice I pass along is.

And this is also I should say something that was done in this instance, is reach out to experts. There are experts around and it's easy to find them who have expertise and can guide your organization through this. I'd offer that expertise to people that have experienced the cyber-attack. I'd also offer it to anyone who investigating a cyber-attack. Now, not you because you've already done that, you've already investigated cyber-attack before, but any of my other colleagues or any other organization that has to do the investigation also reach out to experts.

And we were lucky enough, one of the first calls I made was I talked to you about it, about your experience and I looked at your report. And also, I reached out to the Office of the Privacy Commissioner and talked to them and got their expertise. We hired technical experts to help us with the technical aspect. We talked to the Office of the Privacy Commissioner to help us find those technical experts. This is not the time to try to do this on your own when you're suffering a cyber-attack, look for help. The last thing I would focus on is during the immediate aftermath of an attack, an organization is going to experience communication issues of a significant type.

So, one, they're going to be trying to figure out how to notify. And again, our general advice is yes, the legislation generally says notify at a reasonable opportunity. Our interpretation is don't interpret that too narrowly, people need to expect to know and need to know, it's material to them. But the other communication problem that's a little less obvious is when you suffer a cyber-attack, there's two problems that an organization is facing. One is, assuming here we're talking about a ransom attack.

They're dealing with the bad actors and they're trying to figure out who these people are and what they want and how to deal with them. At the same time, they're trying to understand that the scope of the problem. In our jurisdiction, the minister called that the law enforcement response, right? Even though it wasn't always a law enforcement response, but that was dealing with the criminals, that's one thing. But the other thing that's happening is a significant operational problem. Because the way that you find out that you've been hit with a cyber-attack is your system stopped working all of a sudden.

This is what happened here is that one day on a Sunday, everything stopped working, because the way that ransom attacks in particular work, they take your data and they lock it down so your systems don't work. Your operational people are trying to figure out how much data they've lost, and then usually there's backups. So, they're trying to figure out, "Okay, we need to get our systems back up and running. We need to restore our data and we need to figure out how much data we can get back from our backups and how much data loss there's been."

So that organizational response, this was our whole health system went down, which is that's a significant province wide crisis to have your whole system with lives on the line. And so, your operational response people are trying to do all that while your law enforcement activity, you're dealing with the criminals are happening over there. This can go on for a period of time, which can vary. The people on the operational side, they're going to be wondering what's going on the other side, and there's going to be real communication problems between the two.

The people on the operational side, they don't really need to know, and they probably shouldn't know everything that's going on the side of the dealing with the criminal's part. But they don't know what they don't know, and they are convinced that they need to know more to be able to do their jobs. There's a kind of fog of war situation that settles in. Organizations need to be aware that that is going to happen. And to the best extent possible, the leaders of their organization need to be aware and ready for that and understand roles and responsibilities, but they also need to understand that as best as you can to prepare for it.

And I think military commanders would tell you that you can understand roles and responsibilities yourself, but you also need to know that there is going to be a fog of war and to understand that that's going to happen and live with it and deal with that. So, I think those are some of the higher-level pieces of advice that I'd share that were real learnings for me from this process. One more general health administration level thing, and one of the things that I learned in health administration is it's a line that comes from journalism, if it bleeds, it leads. This is what is appealing in a journalistic context.

It's also very appropriate in a health context as well. Things like information technology and information management, they are third, fourth in line at best when it comes to getting new resources from the health system. New resources in the health system tend to get sucked up by ever-increasing drug costs, human resource costs, and then people who want more services. So, those three things, the expansion of services, human resources and drug costs are constant upward pressure on health budgets that are already subsuming, in some provinces half of their entire budget.

So, what can be done? How can we then come forward and say, "You got to make cybersecurity a priority?" Well, here's what happens when you don't, because our modern health systems are health information systems, and when the health information system goes down, it all collapses. And so, all of those health services that were at the front of the line, they don't work if you don't have a functioning health system, they also don't work if people don't trust the health system. And-

Ron Kruzeniski:

True.

Michael Harvey:

... people are not going to trust your health system if their information in it is not secure. And we have a much bigger problem if Canadians stop trusting their health system.

Ron Kruzeniski:

Well, Michael, this has been amazing. I think this has been a real education for me and I hope a real education for everybody listening, and particularly I hope people in the health sector listen to the discussion that we've had here. And I hope all of them also read the report because I think it would be really helpful. So, I want to thank you for the time, number one in preparing for this podcast and I know you've put a lot of thought into it and taking the time. Thank you very, very much for doing this.

Michael Harvey:

Well, it's a real privilege, and I do hope that in my small way I can contribute to an improved health situation and security situation in the country. And I really thank you for helping all of us in doing that and your leadership at our table in helping get the word out and advance these principles.

Ron Kruzeniski:

Thanks, Michael.

Michael Harvey:

Have a great afternoon.