National Committee on Vital and Health Statistics
Subcommittee on Privacy, Confidentiality, and Security
Hearing on Security in Healthcare

Transcript

July 14, 2021, 9:30 a.m. – 5:30 p.m. ET

VIRTUAL

SPEAKERS

NCVHS Members		
Name	**Organization**	**Role**
Melissa M. Goldstein	**The George Washington University**	**Co-Chair**
Jacki Monson	**Sutter Health**	**Co-Chair**
Nicholas L. Coussoule	**Horizon Blue Cross Blue shield of New Jersey**	**Chair-Full Committee**
Tammy Banks	Individual	Member
Denise Chrysler	University of Michigan School of Public Health	Member
Jamie Ferguson	Kaiser Permanente	Member
Vickie M. Mays	UCLA	Member
Valerie Watzlaf	University of Pittsburgh	Member
Wu Xu	University of Utah	Member
NCVHS Staff		
Name	**Organization**	**Role**
Rebecca Hines	HHS/NCHS	Executive Secretary/Designated Federal Officer
Rachel Seeger	HHS Office for Civil Rights	Lead Staff
Natalie Gonzalez	HHS/CDC	Staff
Maya Bernstein	ASPE/OSDP	Staff
Geneva Cashaw	HHS/NCHS	Staff
Marietta Squire	HHS/NCHS	Staff
Presenters		
Name	**Organization**	**Role**
Erik Decker	Intermountain Healthcare	VP/Chief Information Security Officer
Jane Wong	UCSF Health	Chief Information Officer
Sabrina Kidd	UCSF Health	Chief Medical Officer
Denise Anderson	H-ISAC	President
John Hennelly	Sonoma Valley Hospital	CEO

John Guerriero	National Governors Association	Cybersecurity Program Officer
Kevin Fu	Food and Drug Administration	Director of Medical Device Security
Suzanne Widup	Verizon Enterprise	Senior Analyst
Kevin Stine	National Institute of Standards and Technology's Information Technology Laboratory	Chief of the Applied Cybersecurity Division
Julie Chua	Health and Human Services	Security Risk Management Division Manager
Timothy Noonan	HHS Office for Civil Rights	Deputy Director Health Information Privacy Division

Welcome and Roll Call

Rebecca Hines: Good morning, and welcome to the National Committee on Vital and Health Statistics, NCVHS, meeting of the Subcommittee on Privacy, Confidentiality, and Security. I hope everyone is well and safe with all the heat and extreme weather in many corners of the United States at the moment.

My name is Rebecca Hines. I serve as executive secretary and designated federal officer for the committee. Today the Privacy, Confidentiality, and Security Subcommittee will be hearing testimony focused on security in healthcare. One of the great assets of this committee is that it is chartered to convene stakeholders to hear a range of perspectives to inform deliberations and development of recommendations to HHS. So we're grateful to our committee members for your service here today. Thank you for your time and expertise, and to our panelists here today, lending your expertise, knowledge, and experience to inform the members here in this work.

Before we get started, let's take care of roll call. Please, members, remember to state your name, the organization you're with, your role on the committee, and any conflicts. Beginning with our chair, Nick Coussoule.

Nick Coussoule: Good morning. Nick Coussoule, with Horizon Blue Cross Blue Shield of New Jersey. I'm the chair of the Full Committee, and I'm happy to be here this morning, and I have no conflicts.

Melissa Goldstein: Good morning. I'm a professor at the George Washington University in the Milken School of Public Health, I'm a member of the Full Committee, and co-chair of the Privacy, Confidentiality, and Security Subcommittee, and I have no conflicts.

Jacki Monson: Good morning, Jacki Monson. I work at Sutter Health as a vice president, in lots of various job titles, and I'm also a member of the Full Committee and co-chair of the Privacy, Confidentiality, and Security Subcommittee, and I have no conflicts.

Denise Chrysler: Good morning, I'm Denise Chrysler. I'm with the University of Michigan School of Public Health, where I serve as director of the Network for Public Health Law, mid-states region. I am a member of the Full Committee. I serve on the Subcommittee on Privacy, Confidentiality, and Security, and I have no conflicts.

Jamie Ferguson: Good morning, my name is Jamie Ferguson. I work at Kaiser Permanente. I am a member of the Full Committee, a member of the Subcommittee on Standards. I have no conflicts.

Tammy Banks: Good morning, I'm a member of the Full Committee, a member of the Standards Subcommittee, and I have no conflicts.

Valerie Watzlaf: Good morning. I work for the University of Pittsburgh in the department of health information management as the vice-chair of education and associate professor. I'm a member of the Full Committee, and also a member of the PCS subcommittee, and I have no conflicts.

Vickie Mays: Good morning. I'm a professor at the University of California, Los Angeles, in health policy and management and psychology. I am a member of the Full Committee, and the Subcommittee on

Privacy, Confidentiality, and Security. And I have no conflicts.

Wu Xu: Good morning. I'm Wu Xu, with the University of Utah. I'm a member of the Full Committee. I have no conflicts.

Rebecca Hines: Thank you. I believe that's all of our members. So let me turn it over to our lead staff to the subcommittee.

Rachel Seeger: Hi, I'm Rachel Seeger, I am the lead staff to the NCVHS Subcommittee on Privacy, Confidentiality, and Security, and I am senior advisor with the HHS Office for Civil Rights.

Rebecca Hines: Thank you, Rachel. And Maya Bernstein.

Maya Bernstein: Good morning. My name is Maya Bernstein. I am the senior advisor for privacy policy in the Office of the Assistant Secretary for Planning and Evaluation. I'm also staff, the executive director of the committee, and I'm a subject matter liaison to the privacy, confidentiality, and security subcommittee.

Rebecca Hines: Thank you, and also just want to thank our administrative support team here with us, Marietta Squire and Geneva Cashaw. Have I forgotten anyone?

Ms. Gonzalez: Good morning, I'm Natalie Gonzales. I am lead staff of the Privacy and Confidentiality Unit at the Centers for Disease Control in Atlanta, and I am a liaison to the PCS committee. Thank you.

Rebecca Hines: Thank you. For anyone not on the agenda who would like to speak to make a public comment today, there is a public comment period scheduled for 4:30 pm. Note, if for some reason the proceedings move a little more quickly than the agenda outlines, just monitor the afternoon session closely, in case the last panel wraps up early. You're also welcome to submit a comment to the committee by email, and the address is showing here on the slide, NCVHSmail@cdc.gov. We've also already received two public comments, which we will be posting on the website.

With that, I believe we can turn it over to our co-chairs, Melissa Goldstein and Jacki Monson.

Opening Remarks

Jacki Monson: Thanks so much, and good morning. First of all, I'd just like to thank everybody for joining us today, on behalf of NCVHS members, the privacy, confidentiality, and security subcommittee members, and staff. We are very much looking forward to today's discussions. We have a robust agenda that's on display right now. And a lot of topics and panelists who we just deeply appreciate all the time that they've dedicated to this hearing, both in preparation for and the actual hearing today. Of course, to the public and others who are listening, both submitting public comments and also just participating with us today.

This is a very important topic. Every single day, we learn of the impact of cyberattacks on healthcare, including patient safety, technology, infrastructure, the supply chain, public health as it relates to COVID vaccine data, and other COVID data. The list could go on.

Certainly, since the pandemic, we've seen a significant increase in the cyberattacks specifically targeting healthcare. Cybersecurity, in my mind, is a patient safety issue. In order for us to protect the health and trust of our patients, we have to keep patients and their information safe. So we're very much looking forward to learning today about different perspectives on different topics as it relates to cybersecurity, and how NCVHS might be able to help by writing a letter of recommendation to the Secretary based on what we learn today about potential opportunities, either regulatory policy, et cetera, to enhance our ability to really respond to the cybersecurity landscape that we're currently facing in healthcare today.

Just some logistics, as Rebecca mentioned. We will have a moderator for each panel. Each panel member will have the opportunity to provide 10 to 15 minutes of an overview, a PowerPoint presentation, and give us their perspective. Once all of the panelists have provided that time, then we will open it up for Q&A and discussion. From there, we will also have the opportunity, as Rebecca mentioned, for public comment at the end of the day. So if you are a member of the public and want to provide perspective, that would be the opportunity to do it.

Again, I just want to thank you for learning with us today. I can't say that I've ever been so excited for a subcommittee hearing, particularly on a topic that I'm passionate about. Not only in my responsibility as a co-chair for this subcommittee, but it's also my day job to be both a chief privacy officer and a chief information security officer, so I'm very much looking forward to what my colleagues have to say, based on the perspective of what's going on in information security and cybersecurity landscape in healthcare.

With that said, I'll turn it over to Melissa for any short comments she'd like to make.

Melissa Goldstein: Good morning, everyone. We really appreciate your time today. I want to echo Jacki's thanks for everyone coming, our panelists especially, but also members of the public, my colleagues and staff of the subcommittee. There's been a lot of work that's gone into it, and we're very excited to hear form the panelists today and to learn more about this topic.

Security is incredibly important, as Jacki has already said, because privacy and security are interwoven, and we can't work on patient privacy with our healthcare information without working on security at the same time and being able to trust that the organizations that hold our data as patients and individuals are working on security.

So thank you very much, and let's get started. Thanks so much.

Jacki Monson: Our esteemed chair of NCVHS has also joined us today, so Nick, I just turn it over to you in case you want to make a couple of comments.

Nick Coussoule: Thanks, Jacki. No, I'm very excited about the day. It's clearly a very relevant and pressing topic for many of us who live in this world every day and deal with the threats and challenges. So I'm excited for the panelists, appreciate everybody's time and effort going into this. This is clearly, I think, within the quiver of the committee to hopefully be effective at convening a lot of experts and then providing some advice. So I'm excited about it. Thank you all for the work so far and thank you in advance to the panelists for their participation, and the committee members.

Panel I - Addressing Healthcare Security Challenges

Jacki Monson: Okay, with that said, let's go ahead and get started with panel number one. I'll start with brief introductions to all of our panelists and then they can certainly expand on their expertise as they share their viewpoint.

The first individual that I want to introduce is Erik Decker. He is the CISO at Intermountain Healthcare, and also participates in the Healthcare Sector Coordinating Council, and is one of my esteemed colleagues who is really leading the industry as it relates to information security and cybersecurity. So really looking forward to his participation today on the panel.

The second panelist is Denise Anderson. She is the president of Healthcare ISAC. Those of you who are not familiar with Healthcare ISAC, it is an intelligence-collecting jack-of-all-trades, really assisting us with cybersecurity and intelligence data feeds, so we're very thrilled to have her here. She has great perspective, and really bringing not only the big healthcare organizations, but also the small ones into the loop with being able to manage the cybersecurity threat landscape, and they're just a really great advocate for healthcare.

The third panelist is Jane Wong. She is at UCSF as a chief information officer, and I think she'll have a lot of great perspective; as I'm sure you saw in the media, UCSF has been impacted by cybersecurity, and I think they've done a fantastic job recovering from it. So we're definitely going to be looking forward to that perspective, particularly around some impact they had in the COVID data that was tried to be obtained.

Joining her will be Sabrina Kidd. She is a chief medical officer at UCSF, and so really looking forward to that physician perspective on what's going on in the cybersecurity landscape. So looking forward to both of them sharing with us.

Then we also have one late additional add that we're very thrilled about. And that is Sonoma Valley Hospital, John Hennelly, who is the Sonoma Valley Hospital CEO, we've added to the agenda today. Very thrilled to have him. For those of you who may know, Sonoma Valley Hospital was seriously impacted by a cyber issue and ended up having to operate in a paper environment for a long period of time, and some very challenging times for them that they've since recovered from, so really looking forward to John's perspective in sharing how they recovered, and what they're doing to continue to manage the cyber landscape.

With that said, I think we'll start, and we'll start with Erik Decker.

Erik Decker: Thank you very much, Jacki. Actually, if you don't mind, I have some work happening in my house right now, and I've asked them to stop drilling at 9 o'clock my time. But the drilling might happen while I'm doing this. So would it be okay if Jane started?

Jacki Monson: Sure.

Jane Wong: Hi, there. Good morning, everyone. It's really bright and early in California. I just want to make a minor correction of Jacki's introduction. I am the associate CIO, I'm not the big boss, I'm not the

CIO. I'm the associate CIO at UC San Francisco, and with this presentation, if there are questions I can touch on UCSF, but this presentation is really talking about Sonoma and how UC San Francisco is affiliated with Sonoma and myself and Sabrina join hands, and when there was a breach, because Sonoma is affiliated with UC San Francisco.

So I will talk about how we partner and help Sonoma recover from the cyberattack, and also we're going to talk a little bit about our perspective of the challenge of the community hospital, and what does it mean when we have to focus on cybersecurity, and it's really threats for us, and most of the time, with a community hospital, we're spending more time on balancing patient care and IT. So we will show you our challenges, and hopefully maybe you'll all have some wisdom for us for how to deal with some of these balancing acts.

Sabrina, you want to introduce yourself and talk a little bit about Sonoma?

Sabrina Kidd: Good morning, all. Thank you. I am Sabrina Kidd. I am the chief medical officer at Sonoma Valley Hospital. Glad to join you all this morning. I'd like to introduce you all a little bit to our hospital, so you kind of understand the landscape where our cyberattack occurred and our relationship with UCSF.

We are a full-service acute care district hospital, which means we have a public district board. We're located actually in the city of Sonoma, also which is in the county of Sonoma, California. So we are in the middle of wine country, we're about 45 minutes north of San Francisco. We serve a healthcare district of 42,000 residents. We have 24 acute care beds, so we are small. Eighteen of those are medical-surgical and a six-bed ICU.

We are staffed by one hospitalist at a time taking three shifts throughout the day, and there's one ED physician on duty, so we like to think of ourselves as small and nimble, but very mighty. We do have numerous consultants available and growing rapidly with our affiliation with UCSF. Some of these are telehealth-based, which obviously, as we create partnerships such as that, they can be even more impacted by things such as a cyberattack. On site we have general and orthopedic surgery, cardiology, radiology, lab. A few other clinical entities.

Our main telemedicine that are really integral to our survival are neurology, because this is our stroke program, that really works through our ED and is linked to UCSF. So that was very impacted by our cyberattack, as well as infectious disease, which we are also linked very closely.

In our facility but under different management is also a 27-bed skilled nursing facility, so when there's disasters in our house, they usually affect both of us.

As I said, we are affiliated with UCSF. This began in 2018, and at that time it was mainly focusing on shared quality and best practices. In 2021, right in the beginning of January, it officially was deepened, and now includes a management service agreement for leadership. That means that myself, John Hennelly, our CEO, our CFO, are all employed by UCSF, and following the cyberattack, we added an additional position to this management service agreement that we're very excited to get off the ground very soon, which is a director of IT services, that will be also a UCSF employee so that we can better share resources to this community hospital.

Where's our funding come from? I think also, this plays into preparations for a cyberattack, so I wanted share this with you. Largely we have revenues from services, and our population is largely public based. This is a very retirement-friendly area, so a lot of places call this Disneyland for seniors, which means we are largely a Medicare population with revenues for services. We also do have a parcel tax from those 42,000 residents that are in our district. We are fortunate to have a very charitable community, so that is a large source of our funding for capital expenditures and pretty much our only source of funding for capital expenditures. Our operating budget is so small, it doesn't really allow for those, which also really impacts our ability to keep our IT infrastructure up to date.

In order to get our facility up to the 2013 standards for earthquakes and facilities, we had to have a $35 million GO bond. So that's all been spent and done, and in order to comply for 2030, we'll be looking for other solutions. So there's a lot going on for a small hospital these days.

Our IT budget, to give you an idea what we are working with, is about, for this next year, is about $3 million. That's about 5 percent, which is within the healthy range for a hospital our size, of about 5 or 6 percent for an IT budget of our total operational expenses. It was a bit less than that prior to this. We have definitely upped the budget in response to the cyberattack, and this is all security measures that are absolutely mandatory that we implement.

I'll hand it back to Jane to tell you a little bit about UCSF.

Jane Wong: I would just touch on a little bit about UCSF. UCSF is what we call an academic medical center. We are exclusively focused on health, unlike some of the UC University of California campuses. We are only professional schools, so we don't have undergraduates, and our medical center is ranked among the top ten hospitals nationwide. And we have a lot of specialties. With UCSF, what we called a health entity, we have medical center. We also have children's hospital, in both San Francisco and Oakland, and then we have psychiatric hospital and the dental center.

According to US News & World Report, we're the number two in primary care, and you can see that we focus only on healthcare and also biochemistry. We do a lot of research on biochemistry, especially recently with the COVID. We did a lot of research.

As Jacki mentioned earlier, we get cyberattacks every day. We see it, we have intelligence, and a lot of times they are very interested in our research data. So we have very -- we spend a lot of money and a lot of resources on securing our border. So we have quite a bit of intelligence and based on that, with our affiliation with Sonoma, every time if I have new information, I immediately pass to on to Sonoma so that we keep our affiliation also safe.

Let's talk a little bit about the constant threat landscape. As you all know, recently we have SolarWinds, we have Accellion, all the attacks. And especially with the COVID, we have a lot of remote workers. We pivot completely to remote, and with that, all the VPN, all the Citrix, all the remote systems that our workers leverage are being attacked. So this is extremely dangerous and especially concerning for us, because we feel like we are always chasing, and we plug one hole, there's another hole out there. So I hope that there is some consistency across and we share information, so that we are not only fighting this battle alone.

One of the also our experience we found is that the attackers, they break in and then they deliver a payload, and then they get out. So in some of the incidents that we found, they were lurking around for close to a month in our system but they didn't take any action, and they were looking to see whether we catch them and we plug our holes. So it becomes -- we learn a lot of things while we're watching and hopefully everybody can share some of these information.

Also, you know that healthcare now is the third most-targeted industry from a cyberattack perspective, versus back in 2019, healthcare was only eighth. So you can see they are targeting the healthcare industry more and more these days.

Sabrina, do you want to touch on what we have --

Sabrina Kidd: I'll talk a little bit about how our cyberattack started. This occurred in October of 2020. It was a Sunday morning, and it was some unusual network activities were detected, and it initially started with some systems that just weren't acting properly for an early morning for our ED. Our IT team was immediately put on guard, and they couldn't figure out immediately what was going on until they discovered a ransomware note.

At that time, our senior leadership was notified, and our incident command center stood up, and immediately got on an ICC zoom, which we'd gotten very good at that point, secondary to COVID, to start figuring out where to go next.

Immediately all computer systems were taken offline. This was to contain the attack and to surveil what had been affected. We went on a complete downtime protocol. What this ended up being is that for some complicated reasons, we were not able to successfully continue mammography due to not being able to get the reports delivered properly, but all other patient care was actually able to be continued in the old-fashioned paper way with a lot of faxes, a lot of telephones, and a lot of verbal communication.

As you'll see, we actually ended up being on some form of paper for approximately four months. We were completely isolated with no access to even any internal computers, we couldn’t even use basic functions such as email or anything like that if were connected to the hospital, so we had cellphones, and we could use mobile devices if they were using cellular service. But we did not have a network that we could connect to in any way.

We were fortunate to actually have cyber insurance, so we used that to engage our cybersecurity experts immediately, and we were very fortunate to be affiliated with UCSF, and we were able to get connected to Jane and her colleagues, who were invaluable to us in helping navigate and give us resources to try and get our systems up and to organize and focus us in a way to do so.

We also engaged external recovery teams within a week to really focus not just on what had happened and the forensics, but to focus on getting us functional. As part of this, we also had to deal with the breach management and notification with a cyber attorney, so that was another arm of this going on simultaneously. As I said, we had the cyber insurance, fortunately, and they helped navigate us through some of this and connect us with the different vendors we needed. And of course we also did notify law enforcement, although we weren't actively engaged with law enforcement throughout this. We were largely with the private companies at that time.

Throughout all of this, we did a lot of discovery, a lot of debriefing, and we have that this did start with a phishing email. A privileged IT account was then used to get access to all other systems. Some data was encrypted by the threat actors. Primarily the data that they took was related to a migration of our PACS server, which is our imaging server, all of our images, as well as their reports.

We were in the process of transitioning from one PACS server to another, and that was the main data that was encrypted, as well as a shared drive that was used for administrative services, so this greatly impacted administration as well as clinical services. Again, some of that backup data related to the shared drive was unfortunately lost.

The recovery took about four months, as I said. It involved many different teams, working simultaneously and pretty much around the clock to get this done. There were no weekends, and there were late nights and a couple of hours of sleep for most of the individuals involved. This was on behalf of UCSF, the external recovery team, our small IT team of seven staff, plus some extras that we brought in, working around the clock, and many consultants to augment the staff as well. There was a lot of notification that had to be done to all the regulatory reporting at government agencies, impacted individuals, as well as the Office of Civil Rights audit that we completed in the early part of 2021.

Jane, do you want to take this next one?

Jane Wong: Yes, I'll talk about the moving forward. First of all, a few things that lessons learned immediately is education of your end user. As Sabrina mentioned earlier, is how it all started with this phishing email. Definitely, I would advise everybody to make sure your end users are educated and figuring out how to educate them to spot phishing emails. That's where it all started. On top of this, I can say that it was a ransomware attack, but we did not pay ransom. We definitely lost some data, but luckily that most of the data we reconstructed, and definitely there are some data lost that was in the administrative world, and we just lived with that. So we did not dole out any dollars for the ransom.

So, moving forward, what we are doing is we need to make sure that your backup is always -- you do a regular validation that your backup indeed safe and immutable. So it's important that you save your backup somewhere, not just in the same area, because if it got encrypted, then all your data, you don't have a backup.

The other thing was keeping up with the security patches. This is really important, and yet it's a balancing act, because there are so many patches out there, and as I said earlier, you are literally trying to keep up with patches and patches, and with a small hospital, it is very hard to keep up with hundreds of patches.

Then the other thing that we're doing and with utilizing some of my resources on the UCSF side, is we want to build a sustainable plan to avoid end-of-support and end-of-life software and hardware. Because once you reach end-of-life, you don't get any security patches from the vendor. Which is, in this case, it happened.

What we are doing now in progress is implementing the multifactor authentication, and also a secure email, which has happened already, which is a great thing, and then we're doing offsite backup, and we store the backup offsite now. And we also leveraged a vendor now with 24/7 security monitoring, which

is important, because of such a small team, we need to leverage some of the external vendors. And then as I mentioned earlier, more security and education for all the staff.

I will start and, Sabrina, please chime in. As we mentioned earlier, the budget is small from a community hospital perspective, and it's always a chasing game, and so the IT team is small, but at the same time, because we have to support so many different applications, so their knowledge is not as deep, they are broad. This team is mighty, but at the same time, when you focus on very deep knowledge, they cannot, because they have to support all these broad-based systems. So we're relying on external vendors a lot, and the other thing that we need to focus on, which we're doing, is we got approval to get a dedicated security lead, because there wasn't one currently in the existing team. So we got approval for the budget, and it's important.

It is very hard to keep up with all the threat intelligence, and it's a balancing act. The other thing that is important is the security team that I have at San Francisco, we're going to make available a lot of what we found and what we learned through our affiliation, and I think that's part of -- we found that that should be part of our affiliation benefits of helping each other.

So hopefully, with that, we can help the team and stay ahead of all the threats out there right now. Sabrina, do you want to expand?

Sabrina Kidd: Just a little bit. I echo everything I think Jane said, and first looking at what larger, other places could do, what would be valuable to us even outside of even UCSF, is basically we are very fortunate to have this affiliation. However, in structure we're very similar to what's called a critical access hospital. We missed the qualifications by being a half mile too close to another hospital, otherwise that's us.

So we know there's a lot of other very vulnerable institutions who may not have such affiliations to deal from, and if there were larger national resources that could share this information in a secure way, if there were playbooks that helped to know exactly what to do and walk you through the steps when this occurs, I think a lot of it is understanding that paying the ransom is separate from having to rebuild your system, and rebuilding a system just takes time. There's a lot of independent vendors you have to work with, you have to bring together; there's a lot of steps, no matter how well you are prepared, but you can really shorten that time by having it outlined.

Encouraging everyone to have their workflows well diagrammed ahead of time, to have maps, not just of all their IT infrastructure, but also their clinical, to really take a look at your old-school paper plans and make sure they're doable, make sure that your backups aren't stored on a computer somewhere, make sure you actually have printed copies, that you could go offsite and actually make a paper copy of. There's a lot of things like that that I think would help other institutions think through this process. A lot of times we're told broadly, have a business continuity plan, but for hospitals, I think that's a little bit more complicated, and I think a lot of work could be done to actually share with smaller institutions, especially, what that means.

And thinking outside the box, besides just the measure of, oh, sure, we had backups, but a lot of them were on a shared drive, and that meant they weren't useful to us. So you have to think of even more

scenarios that could affect you than just your EHR being down, which is a lot of what people are prepared for. They're not prepared to not be without a computer. And that's the true scenario that you're facing with such an attack.

Jane Wong: On top of this is downtime procedures. I would stress so much on making sure you have downtime procedures, and you practice it. You really have to try and do a dry run of downtime procedures, because that will tell you what you're missing. I think Sonoma is great, that there is some downtime procedures, otherwise it was so tough.

The other thing is password change. I would stress so much on making sure that you have regular password change, because what happened earlier, as we mentioned, is the hacker got hold of a privileged account, and that account password was not changed for a long, long time. So those are the things that I would say, first off the bat, those are easy things, and as Sabrina said, if there is some sort of a playbook that said, okay, these are the top 20 things that you all should be concerned about, I think it will help. It would definitely help the community hospitals.

That's our short presentation about what we experienced.

Jacki Monson: Thank you. Is John Hennelly with us?

Jane Wong: I did not see him.

Jacki Monson: Let's check back in after the next panelist speaks.

Erik, are you ready to go?

Erik Decker: I am ready; the drilling has stopped. Sorry for that delay.

Thank you very much. I do not have a PowerPoint presentation. What I have just a written testimony that I'm going to read and just some thoughts to provide to the committee.

Thank you, everybody. My name is Erik Decker. I'm the chief information security officer for Intermountain Healthcare. Intermountain Healthcare is a nonprofit system of 25 hospitals, 225 clinics, a medical group with 2,600 employed physicians and advanced practice clinicians, as well as a health insurance company called SelectHealth, and many other healthcare services within Utah, Idaho, and Nevada.

Intermountain is widely recognized as a leader in transforming healthcare by using evidence-based best practices to consistently deliver high-quality outcomes at sustainable costs. I'm here today to present on behalf of the Health Sector Coordinating Council, or the HSCC, which is where I serve as an elected member of the executive committee. So on behalf of the HSCC, I thank the Subcommittee on Privacy, Confidentiality and Security for inviting our input on improving our security postures within the healthcare industry and the challenges that we face within our sector.

As you might know, the healthcare sector is one of 16 critical infrastructures that's been identified by the U.S. Department of Homeland Security. The HSCC is the private sector led critical infrastructure

advisory council that was formed under Presidential Directive 21 back in, I believe, about 2015. We represent large, medium, and small healthcare industry stakeholders working with our government partners to identify and mitigate threats and vulnerabilities that affect our sector in order to deliver healthcare services to our nation's citizens.

My summary today for conversation is really going to be focused on four areas. The first one is going to be around understanding the new threat landscape and where things are going. Topics around continued incentivization for the healthcare industry and providers. Our sector response to the threats that are occurring, and some additional policy recommendations that I have.

So let's start off with first understanding this new threat landscape. Historically, the focus of threat actors that have tried to attack healthcare organizations has been related to the theft and sale of sensitive data. So really focused on that data aspect. As our sector has evolved to protect against these data concerns and threats, the threat actors have also evolved. As noted by the HC3 in 2021, there was a total of 48 ransomware attacks that impacted our sector. This was up significantly from the year prior. Additionally, within the last year alone, we're seeing 72 percent of these ransom incidents that are also including data leakage. So not only are they shutting down systems, as we just heard about recently, they're also taking the data with them as they're shutting down those systems, for a two-pronged attack.

Another study has found that there was a 55 percent jump in cyber incidents in our sector in 2020. So we are continually seeing every year there to be more and more attacks and more impact.

According to the joint bulletin authored by the Cybersecurity and Infrastructure Security Agency, or CISA, the Department of Health and Human Services and the FBI, last October, produced a report and a warning about a credible threat of increased and imminent Ryuk ransomware threats to our sector. So if you recall, back last fall, there was about seven or 17 systems that were shut down within a short timeframe, and many other systems that were being threatened by this.

This was quickly followed by the SolarWinds Orion Network Management supply chain threat that was also announced by CISA, and then shortly followed after that by a related Microsoft Exchange Server threat. Just this last fourth of July weekend there was a new supply chain attack that impacted the IT software management company called Kasia, and it's been reported that that particular threat caused impact of up to 1,500 businesses in a single day.

If these threats and these attacks had occurred at the beginning of the pandemic last year, while the health sector was reconfiguring its operations to support a response to the spread of the COVID-19 infection, it would have caused catastrophic impacts to public health. This demonstrates that these threat actors continue to adjust and evolve and cause maximum impact to their victims.

The last several years have taught us that the threat actors will continue to innovate new ways to cause damage and extort our sector. As we consider new innovative ways to protect our sector, we must also consider how the threat actors are changing in tactics, as they have in the past. Today we deal with the issues of data theft and extortion, and it impacts the patient care due to our systems being unavailable. We must consider the ability of the threat actor to hold the integrity of our data at ransom as well.

For example, it was demonstrated through security research recently that malware could manipulate and inject realistic images of cancerous growth into MRI scans. When radiologists looked at these images, 99 percent of them believed that the scan had detected cancer. And there was no cancer within the scan itself. So this kind of attack brings the deepfake to healthcare. And a future attack could extort our very ability to trust the data that we use to treat and care for our patients.

So that is a bit of the backdrop of what we're dealing with. As related to incentivization, we're pleased that Congress signed into law in this past July H.R. 7898. It's now called Public Law 116-321. And this law recognizes the increasing and dire cyber threats against the health systems and our regulatory structure under HIPAA has been skewed too heavily toward penalizing even the best prepared and well-resourced healthcare organizations victimized by these attacks.

The new law rebalances these inequities by directing HHS, when making determinations against HIPAA-covered entities and their business associates victimized by the attacks to take into account a covered entities use of recognized cybersecurity practices during the past 12 months. More importantly, this provision serves as a positive incentive for healthcare providers to increase investment in cybersecurity for the benefit of regulatory compliance and ultimately, patient safety.

Among those best practices recognized by law are those established under section 405d of the Cybersecurity Act of 2015. Section 405d was implemented as a joint standing task group of the HSCC cyber working group and HHS. It's comprised of more than 250 volunteers from the HSCC membership and HHS, and I am the industry co-lead for that initiative. The result of this, which was two years in the making, was a publication called the Health Industry Cybersecurity Practices, or HICP, or as I like to affectionately call it, hiccup.

HICP provides a scalable and voluntary cybersecurity principles and practices for use by providers of any size and ability. This publication is designed to be used across the sector and it's tailored to both the small, the medium, and the large-sized organizations. We're grateful for the support that this new law will provide, and we are concerned that HHS has chosen to publish a request for information prior to the publication of a proposed rule. Adding an RFI to the comment process will inevitably slow the process and add another layer of bureaucracy that we cannot afford, while cyber threats continue to advance and healthcare providers try and keep up. As we know from the past year, many cyberattacks have been successful and have brought some providers to their knees, by forcing them to divert patients to other care settings and dropping down to paper records. These scenarios place patient lives in the balance and drive up the cost of care for the sector.

Per the U.S. Census Bureau, there are 907,426 businesses within the healthcare and social assistance sector. Yet the majority of these businesses operate on very thin margins and consider cybersecurity to be a non-revenue-generating overhead cost, as we just heard from our previous panel, that the resourcing available for cyber is very difficult in the small-size organizations. This means practically that the majority of these organizations underinvest in cybersecurity protections or rely on their IT department to absorb its obligations. Knowing that cyber safety is patient safety, this business paradigm needs assistance.

Given that the Centers of Medicare and Medicaid Services, or CMS, is the largest payer in the United

States, I propose a reimbursement model designed to directly fund cybersecurity programs, that that be investigated. This revenue would help set a minimum floor protection, which is crucial for the public health and wellbeing as we embark on the digital age.

Additionally, the HSCC recommends to this subcommittee, one, that we advocate for HICP and other HSCC best practices, which are freely available tools that can be used by the sector to strengthen our collaborative and collective cyber posture. Two, that we request HHS to directly move to proposed rulemaking for the implementation of Public Law 116-321. And three, that we push for policies that incentivize or reimburse healthcare providers who practice better cyber hygiene rather than punitive approaches that penalize them.

So, our sector is addressing these threats through the HSCC as part of this cybersecurity working group, which is represented by more than 300 healthcare organizations and over 600 members. These members are a part of direct patient care, medical materials, health information technology, health plans and payers, laboratories, biologics and pharmaceuticals, and public health. In the Cybersecurity Act of 2015, section 405c directed the establishment of the healthcare industry cybersecurity taskforce, or the HCIC taskforce. This HCIC taskforce produced a publication back in 2017 that outlined six imperatives and over 100 action items to combat the cyber threats that we are dealing with. The HSCC cyber working group has organized around this HCIC taskforce report and works in partnership with HHS to implement new publications and materials.

The HSCC has made tangible progress towards recognizing and addressing numerous weaknesses in cybersecurity of our systems and operations, supply chains, and particularly to the formation of 15 task groups and the creation of 11 industry developed best practices and guidance, some of which were jointly developed by HHS and the FDA over the last three years.

These resources include protections around medical device product security and management, cybersecurity practices for health delivery organizations based on the NIST cybersecurity framework, methods for tactically managing a cyber crisis, security management of healthcare supply chains, telehealth cybersecurity, and protection of innovative capital such as vaccine research, against cyber theft.

We encourage the continued participation with our sector risk management agency, or the SRMA, which is HHS, as well as other key agencies within the federal government, such as CISA, the FTC, and law enforcement agencies such as the FBI.

I'd like to close with some additional policy and regulatory recommendations. In addition to HICP's best practices that I referenced before, I'd like to spend some time talking about information sharing in particular, and I'm sure Denise is going to talk about this as well when she gets onto her panel.

Within the Cybersecurity Act of 2015, healthcare organizations are permitted and protected to share highly sensitive cybersecurity threat information specifically with CISA, the Cybersecurity and Infrastructure Security Agency. This sharing provides liability protections from regulatory enforcement. Unfortunately, in the midst of a cyberattack, most healthcare organizations will work directly with their respective law enforcement agencies, such as the FBI or Secret Service, and limit further sharing due to

concerns of incident leakage and misinformation.

CISA has asked for more intelligence sharing across the industry, which is appropriate, yet in the midst of a crisis, it's difficult to engage with all the federal agencies in the manner and course in which they desire. It's recommended that law enforcement serve as that funnel to CISA, sharing the threat information directly with CISA in as near real time as possible, so the government can help protect other critical infrastructure.

Additionally, during a crisis, an organization quite often needs to have access to sensitive threat intelligence managed by law enforcement. Unfortunately, law enforcement tends to be hesitant to share this information back for fear of impacting their investigations. That same information is needed by the healthcare organizations to assess its impacts and protect patient safety.

Lastly, there continues to be an ongoing misunderstanding amongst some providers around when threat-sharing is actually allowed. We recommend undertaking an initiative that, a, allows for improved bidirectional information-sharing between healthcare and law enforcement; b, aggregates information-sharing from law enforcement back to the critical infrastructure through the information sharing analysis centers, or the ISACs; and c, provide further education to critical infrastructure around its legal protections for sharing sensitive information with the federal government; and d, provide more education on when threat-sharing is permissible.

I do have additional recommendations written into my written testimony, which focus around Biden's 100-day plan, the support of this new SRMA, as well as continued support for the healthcare sector coordinating council. But I'll leave those into the written testimony. I appreciate the opportunity to present, and I'm available for any questions.

Thank you.

Jacki Monson: Thank you.

Denise, we'll go to you next.

Denise Anderson: Thank you, everyone. I am Denise Anderson. I am the president and CEO H-ISAC, or Health ISAC, as you heard earlier. I'm happy to talk today about the role of ISACs in healthcare and some of the threat landscape that we've seen in healthcare.

So what is the role of ISACs in critical infrastructure security. Basically what we are are trusted entities, trusted communities, where critical infrastructure owners and operators can share information with each other in real time, we're talking about optimal information, timely information, and information that's relevant to them to help protect against threats.

They have really strong reach into our sectors and we have an all-hazards approach. So we're looking at both cyber and physical.

Can you hear me better now? Okay, great.

So we also are very operational in nature. So I like to say we're where the rubber meets the road. When an incident happens, we're instantly sharing information, collaborating with each other, and coordinating with each other.

Most ISACs have global members and global operations. We're all not-for-profit. We are private sector organizations, again funded by our owners and operators of the various sectors of critical infrastructure, and we all collaborate through the National Council of ISACs. There's 27 ISACs that are members of the National Council of ISACs at present. I actually happen to serve as the National Council of ISACs, and I work very closely with all of them, and they serve the various critical infrastructure sectors that serve our world.

A little bit about Health ISAC. We were founded in 2010. We are a global organization, and you can see here that we serve a number of constituents within the health and public health sector. For example, providers are members of ours. We have pharmaceutical manufacturers, medical device manufacturers, healthcare delivery organizations, and the like.

So as I mentioned before, we are a trust community and a forum for information sharing where we're looking at things like situational awareness, knowing what threats are out there, what to do about them. We protect each other. We have a saying that one person's defense is everybody else's offense. We're constantly looking at the threats that are out there, the vulnerabilities that are out there. We share best practices with each other and mitigation strategies.

(Pause for audio issues.)

So just to give you a little bit of stats, in 2020, we did almost 800 victim notifications. We put out a number of threat bulletins and vulnerability bulletins, and then we shared almost 200,000 independent indicators of compromise, which are things like IT addresses, email addresses, other tactics that are used by the threat actors to tap into them.

This is just a general idea of how we share information. So if you look at the left side of the screen, you could see the various sources of information that come in and then in the middle, the members are our main source of information. So when an incident happens, at a member organization, they're sharing the information back into the top, which then gets pushed out, as you see on the right side of the slide, to our members. As much as possible, we try to push it out to the public. We push out to the trade associations and other partner ISACs as well as our government partners and law enforcement. So this is very important and we play a very centralized role in getting that information out to everyone.

(Audio drop.)

Denise Anderson: So do you need me to repeat anything I've gone over previously? Or did you catch everything?

Jacki Monson: The last slide would be great, thank you. Thank you, Denise.

Denise Anderson: No problem. So these are the types of things that we share in the cyber realm. We also share very similar type of information in the physical realm. So for example, tactics and techniques

and procedures that a threat actor would use from a physical perspective. So again, as I mentioned earlier, we're an all-hazards focus. So we look at both cyber and physical.

You can see the variety of ways that we share information. So we have a portal with alerts that we push out to our members. We also have list servers and secure chat platforms which are very active, and when an incident happens, people are chatting immediately about it and sharing information with each other.

We have automation. So that's machine-to-machine sharing, where machines are automatically sharing indicators to other machines, and Health ISAC was one of the first organizations to adopt automation, and we have a very robust protocol as far as the automation is concerned. We have briefings that we conduct. In fact, today we are doing a briefing on some of the various threats that are out there, and as things break, we'll stand up a briefing and get that information out.

We have daily products and alerts, and I'll show some of those a little bit later very briefly. We do a monthly threat briefing for our membership, and we also do a cyber threat level every month or as needed if an incident breaks and we need to change the threat level.

We also try -- we abide by the traffic light protocol, so TLP. That's a very common way that we share information. It actually helps people understand how it can be disseminated. So if it's TLP red, it can only be shared with a certain group that is specified in the dissemination. If it's amber, it can be shared a little bit more broadly. So for example, in the case of the ISAC we share with our members. Green gets shared with trusted partners. So it may be government partners, other ISACs, that type of thing. And then white is open source.

We try to bring as much information as possible down to the TLP green and TLP white level, and we try to push out stuff through the website for all of the public to see as much as we possibly can.

So we do daily reports, as I mentioned earlier, both cyber and physical. We conduct a variety of surveys so the member will come to us and ask for some questions, and we'll push that out and conduct a survey. We have tabletop exercises that we do and of course as a result of that, also after-action reports. We have a Patch Tuesday podcast that we do with Microsoft, and actually, I believe that we had a webinar yesterday with Microsoft, around some of the print nightmare vulnerability that's out there right now.

We do a weekly indicator of compromise report manually, although we're also doing that constantly through automation. We have a blog that we do weekly that looks more at the policy legislation issues within health called Hacking Healthcare, and then we put out a number of partner reports from our partners like Flashpoint to the sector to our members.

There's also a number of white papers that we push out, and most of these are available on our website. So we've done a series on identity and access management. So you could see that there. We've also done some papers on insider threats and cyberespionage, and the one on the left there is the strategic threat intelligence on the next SolarWinds event. It's actually a very useful report. I would encourage you to go to our website and look at it if you haven't seen it already.

We also do a lot of networking and collaborating. So we have summits that we put on. We do two summits in the United States a year. We also have them internationally. So we do one in the EU and one in Asia-Pac. We have a number of committees and working groups. I believe the last count there was 27 right now, looking at various topics. They could also be community. So for example, our medical device information sharing council, and others that are on topics like data loss prevention.

We have a bunch of community shared services. So these are tools that members can use across the community, and we conduct a number of exercises to help our members be prepared and look at various topics and issues.

So I was going to get a little bit into the threat landscape for the health sector. Actually you're going to hear a lot of similarity between what Erik just talked about and what I'm going to talk about, but that's good, because we're on the same page. But do you remember, it wasn't too long ago, that we were looking at paper charts, right?

And now we're looking at an environment where we've completely upended the paper world and we've moved into the electronic world. So everything, even treatment is being conducted electronically, paper, data is being conducted electronically. Images are electronic and being shared in a new way.

And one of the reasons that came about, and I'm pointing here to the rabbit, so back in Australia in 1857, they didn't have rabbits, and a wealthy gentleman brought 13 rabbits from across the globe to his estate for hunting, because he thought that would be great. Within 50 years, they had 200 million rabbits that became a plague that destroyed crops and caused a bunch of other problems in Australia.

Likewise, we had the HITECH Act of 2009, which I'm sure all of you are familiar with, and that was a great idea, right? It made data more efficient. It made treatment easier. It was a great thing for everyone. Everyone had access to their own records. And there was a lot of financial incentives and penalties that were put in place to make sure that medical providers moved data to electronic formats. And there was a great focus on data and privacy.

However, there wasn't a focus on cybersecurity. So that created a huge threat surface that the threat actors realized healthcare had a huge trove of data, and the data was valuable. I came from the finance and banking sector, and obviously financial services has long been a target of the cybercriminals, because they had data and they actually had moved to an electronic format much earlier than healthcare ever did.

And when the threat actors were able to see that, hey, this is really valuable data and now we can access it, it obviously created a threat. Of course, the technology evolution, the fact that medical devices can be connected to the internet, we're actually treating people with technology in ways that we have never done it before and will continue to do, obviously created a huge threat service.

The actors and the threats evolved. So the threat actors went from very simple attacks to very complicated and unique types of attacks that have made it very difficult to defend against, and then there's the nature of healthcare. As I mentioned before, moving from paper to data, connecting things to the internet for access and ease of use and efficiency, the portability of data, which is very unique to healthcare and for example, in finance, Wells Fargo does not -- my savings account at Wells Fargo is not

shared with my checking account at Bank of America, right?

So in healthcare that's different. We have data that's being shared with providers, pharmacies, payers, labs, radiological, hospitals. So it's constantly moving, and that creates an issue. We have a lack or we have had a lack of expertise in cybersecurity within healthcare obviously, because they were doctors and business administrators and not cybersecurity experts. They didn't have to be back in the day.

Very thin margins. So when you're looking at an MRI machine, replacing that, or are you spending a dollar on another new tool that you could devote to patient care. Those decisions were being made where you weren't going to be replacing things that probably weren't being supported any more versus being able to enhance patient care.

The 24-hour operations. It makes it very difficult to take devices down to help patch them or other things within the environment. It also makes it hard to actually do things like training and those types of things.

Very open environment. So patients walk through hospitals, for example, and potentially could access different devices that are out there. There's a very heavy compliance culture. So looking at a snapshot in time and complying against that, but not looking at real-time which our cyber threats are real-time events that we have to be constantly on top of.

And then obviously the silos between the various divisions and staff and actually one of the eye-opening things to me when I came over to health was the divisions between medical device manufacturers and healthcare delivery organizations.

And then we have the incidents. So back in 2015, we had the first attack against data in healthcare, which was the Anthem breach, and millions of records, tens of millions of records, were lost in that breach. Then we moved to where we had continuity and operations and accessibility attack, and that was in 2016, January, Hollywood Presbyterian, which you can see there in red in the middle. One of the reasons I put that in red is because what happened was they paid the ransom and they were public about paying the ransom, and that put a target on healthcare. Immediately, threat actors realized that they had a huge opportunity to collect money, and it's just evolved since then.

Then you had in 2017 the two incidents there on the top right, NHS and Nuance, for example. So that WannaCry and Petya NotPetya, and those were nation-state attacks and third-party attacks that impacted healthcare with downstream impacts like -- and I put Nuance there because Nuance -- actually, I don't know how many people are familiar with Petya NotPetya, but it was a third-party against the Ukraine, a company that did financials for any company that did business in the Ukraine. So there were a number of companies that got impacted because of that. Nuance was one of them.

When Nuance had connections to some of the hospitals here in the United States, they got infected as well. So there was a lot of cascading impact from an attack.

And then of course you see there at the bottom the Colonial pipeline, and this is where you have just seen the targets constantly now changing where they're impacting critical infrastructure that can have wide-ranging impacts. So when you can't have access to gas, that can cause a problem, fuel, that can

cause a problem for operations, for not just us driving automobiles, but for hospitals. Suppose it's a hurricane and we need to fuel generators, those types of things. So it's something we have to be constantly on top of.

And you can see, this was put in comparitech.com and it shows the number of attacks and they've just been increasing year over year. In 2016, there were 36; 2017 53; we did drop down in 2018, but then 2019 and 2020, the number has risen astronomically, and you can see obviously in 2021, we're on track to grow that number again.

And the trends have evolved. The targets have evolved, as I mentioned. Back in the day we had mom-and-pop shops or the original ransomware attacks were against people that had pictures on their computers at home and they would pay a ransom to get their pictures back. It evolved to municipalities, educational institutions, and law enforcement, and we saw healthcare obviously become a target after 2016.

It's gradually evolved to where they're now going after MSSPs who then impact many other organizations that utilize their services. So they're constantly changing their targets. It's become a very specialized marketplace. There's now what they call access brokers that can help provide access to organizations to have threat actors, MSSP is a managed services provider. So they manage the services for other organizations. For example, you might have an internet company that manages the services of your hospital, for example, instead of hiring an IT staff to do it for you.

The specialized marketplace, as I mentioned, they're also crafting emails. They're creating the malware, they're creating the encryption packages. So they've become highly specialized in what they do, and they offer ransomware as a service as one of those marketplace items.

Erik talked about this a little bit earlier. You can see where they've gone to change not just from encrypting data but also extortion by threatening to publish it, threatening to do a distributed denial of service attack, which allows you not to have access to your internet basically, in general terms, and then they have done a reconnaissance of networks, and we're seeing that the prices are climbing for the ransoms themselves.

Of course, there are other threats, not just ransomware. We have the third-party risk. This was one that was really concerning to me, and I think we see this through many of the attacks that are happening now with the SolarWinds, where a lot of us are concentrating on certain vendors, and if that vendor goes down for whatever reason, we all become impacted by that.

Insider threat is a huge issue for many organizations. Blended threats. So that's the physical and cyber aspects. Business email compromise is another one that's not going to go away. Phishing, of course, is one of the most used vectors for attacks.

So we've evolved. It's not just about data. We've seen data manipulation, data wiping, and being able to deliver services. It's become a patient safety issue.

And as I said, we originally were looking at data security attacks. We now are seeing data availability attacks, and my greatest concern is data integrity. Erik talked about this a little bit earlier, that when

you change a record, a patient record, and you see that the blood type has changed, for example, and you don't know it, that obviously can cause huge problems.

So what can we do about this? Certain number of basic things. So for example, an enterprise risk management approach, looking at what the crown jewels are within the organization, what you absolutely need to protect, and then going out from there, and also factoring in how long you can go without those crown jewels if they, for example, get compromised.

Understanding your threat surface and the whole environment and how it impacts you. Getting the board and executive level support and commitment to doing these types of things to help protect the organization. Creating patching and budget cycles that will help support cybersecurity. Looking at threat intelligence, situational awareness, and information sharing for being aware of the threats and how they can potentially impact you. And best practices for how you can protect against them. Doing ecosystem training for not just your organization but your vendor organizations, your partner organizations. Creating total awareness of the threats that are out there and things they need to look out for and be mindful of.

And then breaking down the silos within organizations so that people learn to share, and across organizations, because if you look at all these problems, a lot of them are not technical. They are people problems and process problems, and in a lot of ways they're easy, sometimes complex, but fairly simple to fix or address.

So in conclusion, just a couple of little notes here. One is we still have old threats. We still have those romance scams from Nigeria, because they work. People fall for them all the time. So we can't ignore what we've had in the past. We have to protect against those.

But we also need to stay abreast of the evolving threats, and they're constantly evolving. The threat actors are always looking at ways to attack. It's easier obviously to attack than to defend, and we need to be always two steps ahead of them if we can be.

Taking an all-hazards, enterprise risk management approach to looking at all factors in an organization, and cyber is just one of those, but also physical consequences, other consequences. For example, when the grid went down in Texas and how that impacted healthcare during that time. That wasn't just a cyber problem. It did create a cyber problem, but it also created some patient care problems.

Looking at the cascading impacts and the whole ecosystem and how it can impact you. For example, as I mentioned, the Colonial pipeline attack, when there was no fuel availability, there could -- if there's a hurricane going on or if there was some COVID surge or whatever the case may be, that could also have other kinds of impacts on patient care.

And obviously we're all on the same team. We all need to be working together. Together we stand, divided we fall, as I like to say. And of course, sharing. I would be remiss not to say that we need to share, and shame us for not sharing. There's a number of reasons that we come up with on why we can't share. We need to tear those reasons away, because we need to help each other. The threat actors share with each other. We need to be doing it. And shame on us if we don't.

So that I think is it for me. I will be happy to stand by for any questions. I apologize for the verbal logistics today.

Jacki Monson: Thank you so much, Denise, and we can hear you great now. So I think we solved the logistical challenges.

I'm now going to move to the Q&A portion. I just want to thank the panelists for their formal remarks, and I'm actually going to start with John Hennelly to see if he has any comments that he wants to make, but my question is this. If you were sitting in our seat as the Subcommittee on Privacy, Confidentiality, and Security, what would your top two wish list be if we were writing a letter to the Secretary, which we obviously plan to do, as far as recommendations? What would those two be?

So I want to start with John, and then we'll move through the panelists.

John Hennelly: Thanks, Jacki. I appreciate it. I am actually going to defer that question to Jane Wong, who is way more on this and aware of what's going on. I acknowledge the importance, but the input from her is going to be way more valuable.

Jacki Monson: And John, is there anything formal you'd like to say, since we are hitting you on the tail end of the panel?

John Hennelly: No more than has been said. I'm fully in agreement.

Jacki Monson: Okay, thank you.

Okay, Jane, take it away.

Jane Wong: So I would say the first thing is, as Sabrina earlier said, it will be great to have a playbook that we can share, and I wholeheartedly support what Denise said. Sharing is important. Everybody knows pieces, and if we can have some sort of a sharing and in a secure manner, right? So that everybody can know what am I doing, how can I prevent certain things happening?

So that would be my ask is having a playbook and also have like a solution center that we can all go to and ask questions and get guidance. I think that will be so helpful from a government perspective.

While I have this forum, I would like to ask Denise a question of what she just said earlier when the print nightmare, since it's so fresh and on our mind with Microsoft, would your organization be pushing Microsoft for fixes? Because what happened to us is we immediately disabled all the print, but then Microsoft did not have a fix. The first day when we know that is happening, Microsoft did not have a fix. Would you think that us as an entity we all pushed the vendor, right? Even with SolarWinds, with Pulse VPN, all of those, we should use the power of us to push the vendor. If we are buying the software, they should deliver -- they should be ahead of us.

Denise Anderson: Yes, I agree, and we certainly have relationships with the various vendors, and we certainly have those kinds of conversations, but also just the sharing that happens within the organizations. So there's been a number of threads on print nightmare and the various actions that

people have been taking, which will help everyone. So the community helps itself. But I also think that putting the community pressure on those vendors like Microsoft is very important, and it is certainly something that we do.

And we also try to bring them to the table to like webinars or other types of events like that where they can chat with the members and members can raise their concerns with them and they can hear the collective voice saying you need to fix this. Hopefully that answers your question.

Jane Wong: Yes, thank you.

Jacki Monson: Erik or Denise, other thoughts on my question?

Erik Decker: Yeah, I'll start. I think there's two specific things that HHS can do. So first of all, more support within the operating division that represents the sector risk management agency. So that operating division is ASPR, and right now for facilitating across government, all the government OPDIVs, there is about one and a half, maybe one and a quarter, FTEs that are supporting that. We can do a lot more -- partnership-wise, within industry to HHS, if there could be more dedicated support from within HHS to facilitate between the FDA, the OCIO, the ASPR divisions, HC3, et cetera. I mean, there's a lot of different areas, ONC, other different areas that are focusing on cyber, but as sort of that coordinated effort that is an area of focus that could be useful.

The second one that I would recommend is really getting to the implementation and rulemaking for Public Law 116-321. So if we could -- I know that there's some bureaucratic processes that have to go through -- if we could bypass that request for information and go directly to a Notice for Proposed Rulemaking, it would be great, because there's a lot of folks that are waiting to see what it means for OCR to actually implement this new law.

Or they don't even know that it exists, and that would actually go a long way if OCR actually has proposed their rules and they can work on adopting some of those recognized cybersecurity practices.

Denise Anderson: I could chime in, too, I guess. I would agree with Erik on the resource issue. But I also think it's a true partnership, and I think what we see a lot of times is we're operating in silos and we're not working together, from a public/private perspective, and one of the things I constantly -- harp is a strong word I guess, but harp on is the fact that we need to be working together. There's a lot of expertise within the private sector, as well as in the public sector, but where we can do joint briefs versus just a government brief, where we can jointly do papers and products on various threats or other types of information that might be useful to other organizations. I think that that's something really key is that mindset that we need to be working collaboratively and coordinating together when incidents happen.

Jacki Monson: Thank you. So I'm going to open it up to the subcommittee members if you want to raise your hand if you've got questions.

Melissa Goldstein: Hi, I'll go ahead. First, thank you all for these great presentations. Very helpful. A lot of information that will help us in our deliberations and in coming up with and deciding recommendations to the Secretary, which is our essential role.

So Erik, I actually have a couple of questions for you. With the understanding that a request for information serves very different purposes than the Notice for Proposed Rulemaking, I'd like to know a little bit more, if you could flesh out the idea. So I know that from your testimony, your organization has put together a report with information to be considered in an NPRM. But I'm wondering, you know, an RFI is issued in the Federal Register and is supposed to go to everyone, right, about gathering information, and it's a very typical thing that agencies do to gather information before putting a rule together.

So my first question is about the RFI and what information -- how would you suggest that the government go forward without gathering that information?

The second question was, to pick up on the law enforcement information that you were talking about and the sharing of information between I guess the sector and the industry and law enforcement on the other side, with an -- I'd like to know more about that. I'm assuming that you want bilateral information sharing, but obviously law enforcement is going to have classified information that cannot be shared with the sector. So if you could flesh that a little bit, I'd find it really helpful.

Erik Decker: Yeah, so I think the biggest issue related to the RFI and Notice of Proposed Rulemaking, there is a feedback phase for the Notice of Proposed Rulemaking where the sector can provide its comment back, and so it's really just, it's about how quickly this is going to get done. That's the biggest concern. It's not so much like that we're ultimately concerned that they're trying to gather information. It's we have these threats that are continually hitting us.

There are a lot of people that don't know about this new law that it amended HITECH, that it put recognized cybersecurity practices into the mix. They don't know what those recognized cybersecurity practices are. As the industry lead for the 405d task group, we spent three years of work on this, educating and going through all kinds of angles and resource angles and still it has not hit the sort of critical mass.

So I think it's really just about do we have another 9 months, 12 months, of process while the threats are hitting us. That's really the basis of the comment. I can't speak to exactly what the underpinnings of how OCR, what they know and what information they need to gather. So there is that. I do know that they have access to industry experts and they can ask questions and inquire.

On the second piece, the intel sharing. It's really interesting. So I totally understand and agree to the point of when conducting an investigation, there's a lot of classified information. I actually think that we probably need to rethink a little bit about how the bidirectional component of this works. So maybe there should be clearances or something like that that are offered to CISOs and healthcare organizations or other critical industry so that we can allow for that information sharing to occur.

When a largescale incident is happening, we engage with, you know, be it either the FBI or the Secret Service, depending on what the situation is. They will assist. They will help us in the process, but as we're trying to evaluate what's the scope of the damage and how do we find the threat actor, they have access to information we do not. So we're on the defense trying to figure out where are they? Where are they going? What are the indicators? How is it moving around? Unless you have clearance, if you

have clearance you can get the information from them, but if you don't have clearance, they won't provide it.

And I understand, you know, back to the perspective of the investigation and how important that is, this is kind of why I was proposing be it either it's clearance back with the CISOs so that we can have access to it directly from law enforcement or we submit it back through in real time through the ISACs and through the federal government and DHS. But it has to go in real time. It has to go fast in order for us to be able to actually get access to this information and use it.

I would suspect if the aggregate of that information going back through the ISACs would also not be of interest to the FBI, because it could expose their investigation if some of those indicators were out there. So it's a big challenge. It is definitely kind of a one-way street. You'll get a little bit of information from them. You'll get a little bit of details about who they are, what their intentions are, kind of where they're going within who they're attacking, but as you're trying to make sure you've got everything covered up on your side, you've got a safe operating environment of care, it can be a challenge.

Melissa Goldstein: Thank you. Very, very helpful.

Jacki Monson: Denise?

Denise Chrysler: Thank you so much, every member of the panel. I found myself taking notes not about the complexities, but about all the simple matters that just even people like me, and just the comment about Sonoma Valley Hospital, that all started with a phishing email. I get those constantly, as all our employees do, and thinking security always means huge moneys, huge investment, and yet often it comes down to just us.

I wanted to ask about the term breaking down silos. Denise, you especially talked about this, and we hear about constantly and especially with regard to the COVID pandemic, the importance of breaking down silos and the interoperability, which to me is always sharing information, transferring information, yet when I think about silos, I always think for security, silos good, compartmentalized data. Could, Denise, especially you speak to that, and possibly other panelists?

Denise Anderson: Yes, so there are different techniques as far as when cybersecurity from a technical perspective is creating firewalls and if there's like, for example, an MRI machine that is probably on a Windows 7 platform and is not supported anymore, isolating that device from the network as much as possible or building protections around it. So yes, from a technical perspective there are certain things like walling off or siloing off is important.

But I'm talking about people and process. So people clicking on phishing emails, for example, and the more we can create situational awareness and have them understand the impact of what would happen by clicking on that email and potentially bringing down an incident into an organization, much like that was talked about, Jane talked about earlier, the better off every else would be.

We have silos between clinicians and other departments. We have in the medical device community, there's constant finger pointing between the device manufacturers and healthcare delivery organizations, and one of the things -- it was very shocking to me when I first came over actually, and

we've come a long way in a very short period of time, one of the things that we did was we created the medical device information sharing council which is co-chaired by a medical device manufacturer and a healthcare delivery organization, and both of those entities needed to come together to understand that they both have very similar challenges and they're both on the same team and they need to work together, versus against each other.

So that's one example of breaking down a silo. Getting people to understand that it's important to collaborate and coordinate and work together.

Bringing down silos with the public/private partnerships, for example, is another one where we're on the same team, we need to work together, instead of looking at something from a regulatory aspect, we need to be looking at it from a real-time response view. We also have a big tendency to treat victims as the bad guys, which they're not. They're victims.

So we really need to be cognizant of how we need to work together and communicate with each other about different things that are going on. A lot of people hide behind incidents and won't talk about them. Erik kind of alluded to this a little bit, but when an incident breaks, the lawyers clamp down and won't let organizations share, and that's bad, because we need to be sharing. As I mentioned earlier, one person's defense becomes everyone else's offense. And by sharing the tactics and the techniques that the bad guys use to compromise an organization, sharing those out to the community helps them protect against a future incident.

So those are the types of things that I'm talking about when I'm talking about breaking down silos. Hopefully that answers your question.

Erik Decker: If I could add on to what Denise just said. She's spot on about the lawyers and clamping down on information, and the thing that is -- I think this is something HHS could actually assist with, it's within their purview. CSA, the Cybersecurity Act of 2015, does permit it. There are protections. But there's still a fear that there's a regulatory consequence if any information is shared. So if there could be a position paper or something like that that comes out from OCR, all the regulators, OCR, FDA, ONC, et cetera, on how that information sharing can actually occur, that would be really, really useful.

The other thing I would add from a silo perspective -- although this has gotten a lot better over the last several years -- is the purviews of the regulators, so the FDA is clearly focused on patient safety, medical device quality, et cetera. Those areas. And OCR is very clearly focused on privacy and confidentiality, but we live in an ecosystem where both of those things exist, and when we focus entirely on, say, just a medical device as the specific medical device could cause harm to a patient, the ecosystem can cause harm to a patient and the ecosystem can release data and cause privacy impacts.

So we have to have that ecosystem view from a regulatory perspective, and the FDA and OCR, I would highly encourage them to continue to partner on how to offer some better regulatory enforcement guidance around that concept.

Jacki Monson: Thank you. Val, let's go to your question.

Valerie Watzlaf: Thank you and thank you so much. This has been so interesting and I, like Denise, have

been taking a lot of notes and have many questions. But my main question was for Erik around the incentives and the reimbursement model to fund the cybersecurity programs. So I know this is of course, as you had said, all of you said, is such a major patient safety issue. My question is around do you see this more like being a part of the value-based care model with the reimbursement around these cybersecurity programs, and do you see it also expanding beyond CMS at all or any more of your thoughts on it?

Erik Decker: I don't have a grand plan with it. What I will say is I think the value-based care model is an absolute right way to do it. You know, CMS is -- if we are going to make progress in this -- let me take a step back. The biggest challenge is everybody is fighting for the same dollar, and we can make an argument of a dollar invested in cybersecurity is a dollar for patient safety. Of course it is. We live in a digital environment.

But the reality is that not everybody thinks about it that way yet. So they are putting that dollar into the new tool, the modality, the MRI, the new practice service lines, et cetera. So it's overhead.

But the thought is we have to get to across the industry, we have to get a floor where everybody is up to at least a level so that we can collectively protect our public health. We're a bit in a paradigm right now, and when you go to some conferences, other CISOs will talk about this or you'll hear people say just be faster than the other -- don't let the bear get you. Let the bear get somebody else. The unfortunate thing in that statement is somebody else is going to get got.

We don't want anybody to be implicated by this. So the thought is if there can be a -- and it doesn't even have to be much, just points of a percent, of a reimbursement, that goes directly into a cyber budget, will alleviate a lot of those tensions. It doesn't cause a fight within the organization itself to figure out how to allocate. It's a specific statement about where it's going to go. It would help organizations like Sonoma when we see the budgets that they're dealing with, just percentages are tenths or hundredths of a reimbursement would go a long way.

And then it's up to, after that, it's up to the organizations' risk models and risk postures to determine how else to invest. So that's ultimately the suggestion.

Jane Wong: Can I add one thing? Erik, I agree with you, and I think the other important part is OCR needs to kind of change the model instead of just always penalizing us, have all these fines, threats, to us. They have to partner with us.

Valerie Watzlaf: Thank you.

Jacki Monson: Vickie?

Vickie Mays: Thank you. The question I have is someone talked about some of the difficulties with vendors. So here you are in the midst of a cyberattack, and you need vendors to be able to either give you something and to do it in a very expeditious way. Could you share just a little bit more about what those needs are and could you also say if there are particular vendors that just need to raise their response capabilities so that we have some sense of that?

Erik Decker: I'll put my thoughts into this. So the challenge on the vendor side -- and I will avoid calling out any particular vendor, because it could happen to anybody. So I appreciate the question, but I don't want to disenfranchise. But here's the situation. So we have been moving more and more into the cloud, for all the right reasons. It's better cost of maintenance, better outcomes, better performance, et cetera.

And yet what's going on is that healthcare companies are all sort of converging on the same vendors. So when that vendor -- that vendor, which is part of, very likely part of mission-critical functions of the healthcare organization, if that vendor is impacted, it causes catastrophic downstream impacts. There's been a few of those cases just this year where that's happened. Elekta was one of them. Nuance was the other classic example that happened from several years ago that Denise mentioned before.

The vendor's ability to respond to these attacks and then bring their customers back online tends to be serial. So it's one at a time, and they're prioritizing their customers based on whatever factors they're determining to do that. We all know and we talk about under our business continuity plans and such that having an outage within our digital environment for longer than 8 hours, 24 hours, 48 hours, you start to get hospital administrators and folks getting very, very nervous about the ability to keep up and keep care going and keep care going in a quality way. These outages are occurring for weeks and months when they're happening.

So the paradigm, cloud is not bad. That's not what I'm suggesting. But the paradigm has to include the ability for resiliency around this. So we need alternatives. We need to assume that the vendor is going to go out in some way. So what is the backup associated to that? Is it going to be an on-prem thing? Is the vendor going to have some other failover solution? When we're dealing with mission critical applications, there has to be some other mechanism in place.

Denise Anderson: If I might chime in, too, so the concentration risk is one that is a big problem, I believe, and it's not just cyber, believe it or not. So for example, in pharmaceutical manufacturing, there's certain packaging that is only done by one or two vendors, and if those one or two vendors go down because of a ransomware attack, which did happen, that can impact pushing out vital therapeutics to the public.

So we have to be constantly mindful of the ecosystem and the vendors that we rely upon, whether they're cyber or physical, and be able to build into our playbooks how we will survive as organizations, how we will be resilient if those vendors should go down and for how long, as Erik was just mentioning.

Vickie Mays: Thank you.

Jacki Monson: Melissa?

Melissa Goldstein: I'd like to pick up on the comment, Jane, that you just made and also I believe, Erik, you may have mentioned it earlier, the idea of enforcement by OCR, penalties, versus I guess cooperation or counseling, or essentially that's what I'd like to hear more about, with the understanding that there may be appropriate times and organizations for the enforcement, right? And there may be appropriate times and methods for cooperation, counseling, that sort of thing.

So I'd like to hear more from the panelists about how you envision how this balance may be struck, with the understanding that OCR is an enforcement agency, right? So how do we -- how would you restructure it? What would you think would be helpful to industry, both the compliant organizations, but also the noncompliant organizations? How would you like the federal government agency to strike that balance?

Erik Decker: I think it's, if I could start off, I think the balance is already there. It just happened with the new law, HR 7898 Public Law 116-321. It specifically says if organizations have adopted recognized cybersecurity practices which are NIST-based, NIST publications, adopting NIST cybersecurity framework, et cetera, adopting publications promulgated through 405d that organizations will receive relief around enforcement actions and monetary penalties, oversight, et cetera.

Of course they would have to demonstrate that they have done it for the last 12 months, and I think it's honestly a perfect way of drawing the line in the sand and saying this is what we're talking about when we say due diligence; this is what we mean by due care. Organizations that can demonstrate they've adopted these things that are meaningful ways of protecting patient safety, they're doing the right thing. Don't victimize the victim. You know, organizations that are not, maybe they're not doing the right thing, and I agree with what you said. Enforcement has to happen, and people who are ignoring the problem, there should be consequences associated to that. So that's my take in it.

Denise Anderson: Could we not, instead of fines, have them invest back into their protections, right? So in some way, direct their actions to be corrective, might be another approach that could be more collaborative versus punitive.

Melissa Goldstein: That's helpful. Jane?

Jane Wong: Yes, I think they are getting better, don't get me wrong, but I think they have to appreciate getting more and more understanding of, for example, with Sonoma, there was a breach, and there's still the old way of you have a certain period of time, you have to send us all your protection plan for remediation, while we're trying to still recover from the attack. I think there should be a little bit more leeway and partnership, just take that example. I think they are getting much better, but there are also cases where they have to understand the situation at that time instead of just a blanket of you have so many days to get back to us with your remediation plan, which, yes, the remediation is important, but let's recover first.

Melissa Goldstein: Thank you.

Jacki Monson: One last question, Denise Chrysler?

Denise Chrysler: Sure. I want to use a little care in asking this question, because I don't want to imply it's up to the patient or consumer to protect themselves, but people who are in a situation to compile their own health records, you know, download it from all the portals for all the healthcare providers they see, what are the options for people to do this? Because one thing I think of, for example, you use a third-party app to export and bring all this information together, you have it, but then you have other kind of risk with regard to the privacy of your data.

Erik Decker: So the public health record, the PHR, is that model. You know, it's interesting, organizations like Microsoft used to have a PHR where they were intended to source all of this information so it can be used on the patient's benefit, and then they turned it off. So I don't know if there's really good solutions out there from a PHR perspective specifically for the patient, but I will say that the 21st Century Cures Act and the interoperability rules from CMS are entirely focused on this. So opening up the data, realizing that the data is the patient's data and they want to be able to consume it in the ways that they want to consume it, and I think that was honestly a very good step forward for allowing patients to be able to -- allowing physicians and clinicians to have access to the information that's necessary for the care. It's very common for patients to be consumers and shop their healthcare amongst systems, and so you don't want to have repeat tests and do all of these things that are available in other organizations.

Now there are health information exchanges and things like that that exist. It's not as digitally nice as some of the big tech that's out there and other kind of retail consumer technologies and platforms that exist. But I think it's encouraging and I think we're going there.

Jacki Monson: Jane or Denise, any other comments on that question?

Jane Wong: No, I would say I agree with Erik as the market is getting there.

Jacki Monson: Okay, well, I know we started a little bit early, and so we've got a little less than three minutes left. So I'll just take the time to thank all of our panelists for your time today, really appreciate all of the preparation that you put into it, your well-thought-out comments and your response to our questions. So I just want to thank you and I believe we're now on break for the next 30 minutes until the next panel.

(Break)

Panel II – State, Tribal, and other Perspectives on Healthcare Security

Denise Chrysler: Hi everybody, welcome back to our afternoon session. This morning's panel focused on the healthcare sectors, so I'm pleased to moderate our next session on data security, and this will concern the public sector. All levels of government collect and use sensitive information. This includes to protect people from disease, injury, and environmental threats, and also to deliver and pay for healthcare.

And most of this information comes from the healthcare sector and is shared electronically between healthcare and government. With the government's authority to collect and share information comes great responsibility to protect that data from unauthorized access. In addition to the responsibility to protect its own data, the government serves as regulator regarding the security of data throughout the healthcare industry.

And with that I'm pleased to introduce our two panelists today. First, John Guerriero. John is the acting Cybersecurity Program Director at the National Governor's Association and serves on the Homeland Security and Public Safety Team of NGA's Center for Best Practices, where he supports governor staff and state policy makers on issues related to cybersecurity, including governance, workforce development, and election security.

Prior to joining the homeland security team at NGA, John focused on workforce development, including registered and apprenticeship and occupational licensing as part of NGA's economic opportunity team. John holds a master's degree in public policy and a bachelor's degree in political science from the University of Michigan.

Next, we will have Kevin Fu, acting Director of Medical Device Security at the FDA's Center for Devices and Radiological Health. Kevin is also Associate Professor of Electronical and Computer Engineering at the University of Michigan, where he directs the security and privacy research group. His research focuses on analogue cybersecurity, how to model and defend against threats to the physics of computation and sensing.

His embedded security research interests span from the physics of cybersecurity through the operating system to human factors, past research projects, and include MEMS sensor security, pacemaker defibrillation security, cryptographic biosystems, web medical device security, web authentication, RFID security and privacy, wirelessly powered sensors, medical device safety and public policy for information security and privacy. Kevin received his BS and Master of Engineering and PhD from MIT. And with that I'll turn it over to John, and after our two panelists we will have our questions.

John Guerriero: Thank you Denise. Quite the honor to be here today, as well as serving on a panel full of Michigan Wolverines. Good afternoon everyone, my name is John Guerriero with the National Governors Association. Thank you for having me on today, it's a privilege to speak with everyone today.

For those who don't know, on the next slide I'll just give some background of what NGA is. So since 1908 NGA has been the national nonpartisan association representing the governors across the states, the commonwealth, and the territories.

And so through the NGA governors share best practices and move forward on national and state priorities. And just recently we turned over our chairmanship, so we are now chaired by Governor Asa Hutchinson, and our vice chair is Governor Phil Murphy of New Jersey, Governor Hutchinson with Arkansas.

And then on the next slide I can break down what NGA – So for some context, what we do at NGA is essentially broken down into two separate houses. We have our association side, that represents our membership and advocates for their interest to federal partners on Capitol Hill.

And then we have our center for best practices, to which I belong, which is a separate standalone 501(c)(3) that serves as more the state facing policy consulting shop for governors and their advisors. And then on the next slide I'll break into more of what the NGA center does. So the NGA center offers governors and their advisors best practices and technical assistance on a range of different policy topics shown here.

So before I was part of the cybersecurity program at Denise Mentioned I was actually in workforce development program. And you can see here how our cyber work applies to almost all of these, actually all of them. So I get to know my colleagues pretty closely across the center. And then on the next slide I'll talk a bit about our work here at NGA.

So focusing in on NGA cybersecurity work, our cyber portfolio mainly revolves around the Resource Center for State Cybersecurity, which is cochaired by Arkansas Governor Asa Hutchinson and Louisiana Governor John Bell Edwards.

It's essentially just a network established to provide governors with resources, tools, and recommendations to help craft and implement effective state cybersecurity policies and practices. And I want to spend some time going through the resource center, how we work with states, and then what we've seen from that work with states.

And so on the next slide, so the resource center is more than just a landing page, it's likely more useful to view it as a vehicle for how NGA provides technical assistance to and connects that everchanging network of state cybersecurity leaders.

So this network is more than just a governor's staff or the CIO, the Chief Information Officer, or the Chief Information Security Officer in each state. So in addition to those it's going to be also a network of governors' homeland security advisors, emergency managers, adjutant general in the National Guard, and other state stakeholders, from private sector, academia, workforce development and education systems, federal agencies, nonprofits, and then some of our partner state associations.

And one of the main highlights that we've done here with the resource center is we host a national summit on state cybersecurity where we convene the state cyber advisors, CIOs, CISOs, homeland security advisors, emergency managers, all those that I previously mentioned, we bring them all together to discuss the emerging threats, they learn from each other, and then they also share common challenges, best practices. Most recently we held ours virtually over three weeks in January 21, but the previous one we did in Shreveport Louisiana.

And in addition to that we also hold separate different state policy roundtables where it's going to be a little bit smaller, where we convene a limited number of state officials or attendees, just to discuss pressing issues in cybersecurity. So recently we held one on increasing diversity, equity, and inclusion in the cyber field, and then last fall we held one on cyber-governance.

So in addition to the cyber summit, we also work with states in a variety of ways here as shown on the slide. We do different publications where we work with different partners maybe jointly to produce a piece, like the Center for Internet Security or NASCIO or sometimes we just write one ourselves when we see a pressing need.

Every month we hold a webinar, we have an ongoing monthly webinar series where we really just choose different pressing needs in cybersecurity and highlight either private sector subject matter experts or best practices or case studies in states.

And then separately we also hold one on election cybersecurity as well through a separate grant. So we've been really doing quite a bit of holding one cyber one a month and then also one election cybersecurity a month. Sometimes those topics have a lot of common pieces together.

In addition to that we also do a lot of ad hoc technical assistance. That might be setting up a learning call with two or three states that want to discuss a common issue, or maybe we write up a memo just to talk

through a different research request we received. I would say that the beauty of the resource center is that really any state can approach us with a request and then we'll work towards supporting them on that. There is really no application process or membership really required for some of that.

And then one of the other main pieces of the work that we do for the resource center is a thing that we call Policy Academy. I'll cover this more in depth later, but these essentially are just where we've worked with select states, they went through a competitive application process, and we've worked with them pretty in depth over the course of a year on a set of whatever their strategic goals would be.

And then the next slide, so you kind of have an idea of how we assist states, but I think it may be helpful to have an idea of what we typically assist states with. So the cyber threat landscape is constantly evolving and poses major risks and impacts to state and local government entities. That's not necessarily new news, but over the past three months or so the ransomware, the number of ransomware attacks have really garnered a lot of national headlines.

But before then you didn't have to look far to hear about a government or high-profile organization undergoing a ransomware attack. They've risen exponentially each year against state and local governments. And now we're seeing more frequent attacks against healthcare organizations and K12 school systems, especially with the shift to remote work during COVID.

And even at the government agency side, the shift to remote work, the lines between work and home have really blurred, and just really increases the risks that state networks face. And it means that organization cybersecurity infrastructure is really more critical than ever.

And one of our favorite kind of mottos, if our program had a motto, it would be that cybersecurity isn't just an It issue more, if it ever really was one. This is true on two levels, I think. And first on the organizational side, no longer is cybersecurity really that realm of your IT colleagues or your IT department.

If you have a phone, computer, even a smart device, that needs protection, and it needs cybersecurity hygiene. And its heart, cybersecurity is a human issue, and the solutions are all people oriented. So in observing and adhering to basic cybersecurity hygiene protocols can deter a significant amount of cyber-attacks.

That's simply not clicking on suspicious links or attachments, or setting strong passwords, implementing the multifactor authentication, or reporting suspicious activity, or just essentially knowing what to report and where to report it. That's another issue. But keeping your devices and systems updated as well, just those basic steps can really deter the majority of attacks or attempts. It can increase the cost of each attempt for attackers. But that's on the organizational side.

And then just even thinking on the other side of that, and that's one that we focus here on NGA is kind of at that state level, and what we're seeing is really an increased recognition that state cybersecurity is no longer the sole responsibility of the state's IT department, or the state's IT agency.

The most robust state responses are going to integrate all the different resources that the state has to bear against the threat. So that's going to be the IT department, the homeland security department,

public safety, National Guard, and increasingly also workforce development, education and training, economic development components. And then the nonprofit, academia, and private sector capabilities that states also have to bring to bear.

And as an aside this picture here on this slide I think really elevates that. This was at out 2019 summit in Shreveport, and we have a panel here that, we've got an adjuvant general of the National Guard, we've got a homeland security advisor, an emergency manager, and a state CIO. So really bringing all the different sides of the house together to talk about the cyberthreat.

And then on the next slide I'll go into all of the priority areas that we focus here at NGA. So our work at NGA covers the six priority areas in cybersecurity. So we work on cyber-governance. It's critical infrastructure security. Election cybersecurity, which is critical infrastructure, but over the past year and a half has had its own callout. Incident response planning. State and local partnerships. And workforce development.

And I would say of these critical infrastructure securities, obviously has been front and center the past few months, but also state and local partnerships I would say over the past two years has been one that states are increasingly looking to approach more and more.

And then on the next slide I'll go into what we've been doing this year. So in February or March we launched our 2021 policy academy. So each year when we launch these policy academies we ask states to apply under one, or sometimes more, of those priority areas, except for election security, which was a standalone policy academy in 2019. But in its place there is a fifth catch-all topic that just looks to capture anything innovative states propose.

So here on screen we've got the five states selected, 2021 was really out most competitive bid process to date. We selected Kansas and Missouri under the governance topic, Montana is working on workforce development, and Washington and Indiana are looking to focus in on state and local partnerships. So to be considered each state must include in their application a letter of support from their governor.

So, really right from the start the selected states are working with full governor support, which really helps when looking to convene the very sometimes disparate teams of state and local stakeholders, and this really sets the authority for that work to kind of carry forward.

So through the policy academy NGA works in depth with each state on developing and implementing a strategic action plan around the different goals that they list in their application. We often facilitate really interactive discussions, we build consensus, and help guide the states through that process.

And sometimes the states' goals often change from what they listed in January to where they end up being at the end of December. And so through this academy we are essentially working to support each state to be a pilot state on their respective initiatives that they're looking to accomplish. So essentially just a national model if you will that will have some really good lessons for states in the future to learn from.

And so we have regular check-ins, we do virtual workshops, and then each year NGA staff will go to a state for in person workshops for each state, and then we also convene the leads from each of the state teams together for a monthly cohort call, where they can just share common challenges, best practices, and just kind of have an open dialogue with each other.

And then, so this was the 2021 policy academy, and then on the next slide I'll dive into some of the work that we've done in the past with states on these. So we've been doing on the cyber side policy academies since 2017 or 2018, it definitely predates my tenure on the cyber program.

But one thing is that sometimes outcomes do take time to realize in a state, just given the different legislative and legal landscape in each state, particularly if they're looking to do any sort of statute change. And COVID definitely impacted much of this.

So in addition just to COVID, a lot of our state teams are all multidisciplinary, so if you have a lot of homeland security or an emergency management personnel on a team there is going to be natural disaster response, pandemic response obviously, different things that will definitely draw attention away from the actual policy. But that said, I did want to share with you some high-level outcomes from the previous workshops.

So under the governance category, and one thing just to note here before I dive into this, these are all kind of fluid, the five categories are all kind of fluid, where state and local partnerships have a piece to play in workforce development. And maybe incident response planning definitely has a big part of the governance piece. So some of these are fluid, and I would say that many of these states, they have worked on one or more of these priority areas.

So under governance 2018, the Indiana team drafted a risk assessment tool for local emergency managers designed to help them assess cyber risk at municipally owned critical infrastructure. So the 2018 Policy Academy helped Indiana socialize that tool, with local emergency managers who then agreed to pilot and assist in finalizing that tool.

And then in 2019 we worked with Maryland, Governor Hogan's team, where we utilized their instate workshop as a focus group to vet particular facets of their information security manual, and just gain insight on the best practice programs that they were considering implementing, just various different tools or processes that they were considering. And then we just really worked with the small state team there to really work through their strategic action plan on implementing that.

Under the workforce category, last year we worked with Governor Whitmer's team on establishing a three-pillar framework for building partnerships between the state and K-12 schools in cybersecurity. So the framework essentially looked to develop a maturity model on enhancing school cybersecurity, advancing a K-12 cybersecurity curriculum across the state, and then also cultivating exploration of cybersecurity careers for K-12 students, particularly those in grades 9-12.

Then under the response planning category, last year we also worked with Tennessee, Governor Bill Lee. He had recently established a cybersecurity advisory council that worked with us throughout the 2020 year, just to craft a statewide strategic plan that was non-public. And that plan incorporated the governor's strategic priorities of workforce development and strengthening statewide cybersecurity

among the different political divisions, but also really thinking through cyber-preparedness during a major cyber disruption. So we looked at how to really bring all the different stakeholders together, formulate and develop and continue to revise and refine the state's cyber-disruption response plan.

And then on the state-local side, in 2019 we worked with Governor Baker's team in Massachusetts to conduct a survey in conjunction with the Massachusetts Municipal Association to identify and prioritize the different cyber needs in local governments throughout the commonwealth. So as a result, the Massachusetts team determined that very few municipal governments had cyber incident response plans, and just more generally just knowledge on ways to reduce cyber risk.

So at the in-state workshop in Massachusetts we worked with the team on creating a toolkit designed for municipal government, and then following that workshop the team really carried that forth through a series of different regional virtual workshops throughout the commonwealth to provide that technical assistance on cyber incident response planning to the different local agencies.

And then critical infrastructure security just as an aside, it's an interesting piece, because in many states the ownership of those sectors is not necessarily under the governor's control or the state control. Sometimes it's private sector owned. So it kind of differs by the sector. But in 2019 Louisiana Governor John Bell Edwards' team, they used their in-state workshop to obtain strategic input from the different stakeholders on how the state may incentivize bolstering cyber resilience of their critical infrastructure partners.

So we went down to Louisiana and assisted the team there, and the Louisiana cybersecurity commission in crafting a critical infrastructure cybersecurity portion for their statewide cybersecurity strategic plan, which ended up being non-public, but is still in use today with that LCC, the Louisiana Cyber Commission.

So that's kind of a very high-level overview of the work that we've done with, there are six states there. We've been probably working with upwards of 25 states over the past three years on these policy academies, so there's a lot of lessons to be learned.

But those are probably some of the big high-level takeaways, and I'd be happy to talk more about this work and some of the other work that we've been doing with states, and just other trends that we've been seeing with states as well, in the Q&A portion. I'll turn it back over to you Denise.

Denise Chrysler: Thank you so much, John. And we look forward to hearing more about NGA's resources in the Q&A. Next let's go to Kevin.

Kevin Fu: Glad to be here, thanks for getting the slide deck up there. So great to follow you, John. My name is Kevin Fu, Acting Director of Medical Device Cybersecurity at FDA, effectively on the team that regulates the computer security of medical devices and the safety and effectiveness of those devices.

I'm not going to read my bio. In fact, I think it was already read, so I'll just skip right over that. I think what I'm mostly known for is my early research 10, almost 15 years ago, on pacemaker security. And I just noticed that today is the ten-year anniversary of my last presentation at a federal advisory

committee at the NIST federal advisory committee meeting where I talked about medical device security. So great to be back exactly ten years later.

I also want to point out what I was talking about nine and ten years ago is almost exactly the same when it comes to computer security risks in medical devices. In particular, I talked about the biggest risk was not hackers breaking into medical devices but was instead the widescale unavailability to deliver patient care as well as the integrity of medical sensors.

And I find that really interesting because that was a discussion earlier this morning with some of the other panelists. Of course, we weren't talking about ransomware ten years ago, but we were certainly concerned about the effects of a ransomware-like entity, and that is knowing widescale unavailability was the biggest risk, and it still is today.

We haven't yet seen I would say a lot of evidence for problems with integrity medical sensors, but if my track record is correct it's going to be hitting us in the next few years, I tend to be about ten years ahead of the industry, so I would predict medical device sensors are going to become a big problem in the future. But that's what I was predicting when I was a professor.

So let me put on my FDA hat and give a little briefing about what's going on with medical device security, and then I'll be glad to take questions. So FDA is a regulatory authority, and manufacturers will submit documentation to get premarket clearance of their medical devices, needing to demonstrate certain qualities of their products. And it is a fact that FDA has found some of these submissions to be effectively not cleared for the US market due to cybersecurity concerns alone.

Now, why is that? It's because cybersecurity is safety. You cannot have a safe medical device if it doesn't have adequate cybersecurity from a clinical perspective.

So to address that FDA has been working hard for almost a decade on various documents to guide the industry, to ensure that health delivery organizations can have sort of a good stock of medical devices with cybersecurity built in. Of course, it's a moving target, and it has definitely got a lot of problems worth improving, but I would like to highlight two documents that are really key. One is the premarket guidance document, and one is the post market guidance document.

The premarket guidance document, which is under revision, effectively is about all the engineering expectations that go into a medical device when an FDA reviewer is evaluating the cybersecurity qualities. So it spells out a lot of FDA's expectations. That was finalized almost seven or eight years ago, and today actually will be issuing a new version of this document for public comment later this year expected.

A second document is the Postmarket Management of Cybersecurity in Medical Devices. This was issued about five years ago. This is less a technical document and more of a social and communications document of how do you share information about computer security vulnerabilities and incidence as they relate to medical devices. And that to me is a very challenging problem because it's a much more human problem and a less technical problem.

So as I just mentioned, FDA is targeting a 2021 release of new draft premarket guidance. Again, this is the sort of engineering-oriented expectations, telegraph manufacturers on what FDA reviewers will be looking for in terms of cybersecurity and their design documents when attempting to get a medical device cleared or approved for the US market. That's still on track for late in 2021, and then there will be a public comment period.

One of the biggest areas where there is opportunity to make a real difference with improving security of medical devices is threat modeling. And so to that end FDA has stood up a series of bootcamps to teach the teachers effectively, mostly at medical device manufacturers, on how to do threat modeling. This was through NDIC and MITRE.

Threat modeling, I'll get into in a little bit more, but it's akin to hazard analysis. It's about identifying risks as it relates to computer security, and it's effectively the calculus of computer security, which is quite different from traditional measurement of safety.

Another area that FDA is extremely active in for cybersecurity of medical devices is the International medical Device Regulators Forum, the IMDRF. It is essentially a collection of all the FDAs of the world, of all the different countries, along with representatives for different trade groups, from the medical device manufacturing and healthcare delivery organization communities.

One of the documents that was recently finalized has to do with the total product lifecycle, as it has to do with medical device security, and there's ongoing work, in fact there was just a meeting this morning at seven in the morning, on SBOM, Software Bill of Materials, and getting that language harmonized across all the different regulatory agencies of the world.

So I was getting a little bit ahead of myself on software bill of materials. This is a term that will be rolling off the tongue soon. It was even mentioned in Biden's presidential order on cybersecurity earlier this year. SBOM, Software Bill of Materials, is effectively an ingredient list of third-party software inside a product.

And there's quite a bit of activity in all different sectors of the internet of things, but in the medical device world, FDA is quite active in working on how to use software bill of materials, not just in premarket review and understanding cybersecurity risk, but also HDOs, Health Delivery Organizations, are able to use software bill of materials to better understand their risk when they're installing a device, and it's also very helpful when a vulnerability is disclosed to more quickly ascertain is a medical device at risk in a clinical sense, so you can quickly do triage. That SBOM work is primarily being coordinated by NTIA, and FDA is extremely supportive of the work going on there for this third-party software ingredient list effectively.

As we go down the FDA street of different major initiatives, I want to highlight the joint security plan. We already had mention of the health sector coordinating council earlier this morning. This is just one of the deliverables from that community effort, really bringing together all the different stakeholders, with both an HDO lead and a medical device manufacturing lead.

The joint security plan is effectively the software security development lifecycle as applied to medical devices. So if a medical device manufacturer is somewhat new to security engineering, this is a great

playbook for them to understand how to integrate security engineering into their existing manufacturing processes. But I would say it's an intermediate level sort of topic, once somebody gets their head wrapped around how to do appropriate threat modeling, the next appropriate step is to look at the joint security plan and get that integrated into the manufacturing process.

So threat modeling as I mentioned is sort of the bread and butter of computer security. It's a very proactive approach to computer security, as opposed to reactive, oh my gosh, yet another vulnerability. Why are threat models so important? The reason they're so important is it brings science to the art of defending a computer system, trying to bring more measurability, more quantification.

So it's for instance, it touches on issues of identification and analysis and evaluation of security risks, and this has now been standardized, there's' an FDA recognized consensus standard from AAMI, AAMI is a group representing effectively the clinical side of medical device manufacturing. They have a standard called TIR57, Technical Information Report 57. This was done more than five years ago.

But it talks about for instance how to rank security risks in medical devices as acceptable, conditionally acceptable, or unacceptable, getting to a much more risk management-based approach as opposed to an IT centric approach. Because medical devices are really part of the OT ecosystem, OT sounds for Operational Technology, and that is a term that is also called out in Biden's executive order on cybersecurity, and it's really key to have threat modeling that is respecting sort of the OT-isms of the medical device world. That's because we want to get away from gut judgment assessments of well, we think our device is secure, and move to something that's much more scientific.

So I often like to give good and bad examples of threat models. I'll give you a few bad ones first. An example of an inappropriate threat model would be something like oh, normally we think about medical device manufacturers, but you can also imagine health delivery organizations installing systems, you might make a claim like we use some obscure process, again that's not science, that's not refutable, that's simply a statement of opinion. There might be a claim of something like well we've never been attacked. In fact, those who are not attacked are probably more likely to be attacked because they're letting their guard down. But once again that's not science, and that's not refutable.

A slightly subtler failed threat model would be a permutation such as well, our product must be placed on a secure hospital network in order to be secure. At the outset that seems to make sense, but when you drill down in it you quickly learn that it simply doesn't, because networks are inherently hostile. Even a firewalled network is inherently hostile.

And the real key is understanding how devices can remain safe and effective even when the networks are under the control of an adversary. So I would argue that a reasonable threat model begins with a statement such as well, as the defender we're going to assume that the adversary controls the network with the ability to alter, drop, and replay packets, and then you build your system to be secure despite those constraints for the adversary.

So to that end, we recently submitted a response to the National Institute of Standards and Technology, where they had a call for feedback on the definition of critical software. So you can go to our website,

it's listed down there at the bottom, if you just search for FDA cybersecurity probably that URL will be the first hit, and you can download our short five-page report.

I'll just highlight the first paragraph of our report. We talk about how cybersecurity is crucial for medical device safety and effectiveness. And one of the key things that we point out in our response to NIST is how some of the critical functions are shifting from traditional on premises software to cloud based systems, other remote infrastructure, that can be vulnerable to things like ransomware and other malware that is beginning to rear its head.

And one of the key insights is to realize that firewalls have a very ungraceful failure mode. And so there's a shift in thinking over the last 15 years from this perimeter-based firewall approach to a much more safety centric approach where you need to separate your operational technology from your information technology by design, because mixing the two is going to lead to some unfortunate consequences down the line.

I think I'll skip over some of the engineering a bit for this particular audience, but I'll just say at a high level a lot of the security engineering technology has been solved as of almost 50 years ago. The basic principles have remained unchanged and stood the test of time.

And they can be boiled down to eight basic engineering principles. I'm not going to go completely into sort of professor lecture mode here, but I do want to highlight two of the principles that I think will resonate with the layperson.

First is the fourth principle, the open design principle. In the security engineering world, we advise that you should not depend upon the ignorance of attackers, or depend on security by obscurity, to get any kind of degree of assurance. This is a somewhat counterintuitive principle.

The basic idea is you should assume the adversary knows everything about your system, except perhaps for something small and manageable like the cryptographic key. You should assume they know all your algorithms. You should assume they know all the versions of your software. We're not saying disclose this to the adversary, but as a defender you simply should assume that the adversary is not dumb. And then as a result you tend to design your systems to be much more trustworthy because you rely much, much less on security by obscurity.

A second principle that I think is really key is known as the principle of least privilege, and the basic idea is that computer software ought to use the least privileges necessary to complete a function. So unfortunately, I can't say that's universal today, but with ransomware, ransomware to some extent not following this principle is contributing to the symptoms of ransomware spreading, and for the following reason.

When you run a piece of software as say a supervisor or root, which is like the system administrator, as opposed to an unprivileged user that has fewer access to modify the system, when that software is compromised, whatever is compromising the software will assume all the privileges of whatever the program was running. So if the program was running as a system administrator, it's going to spread quickly throughout that system. But if it's running as a very locked down unprivileged user, it's less likely to spread.

So I certainly hope to see the principle of least privilege, which was coined almost 50 years ago, I really would like to see that used more often in medical device security, because it's one of these opportunities where I think it will eliminate not only known problems and known vulnerabilities, but it's also going to eliminate unknown unknowns, malware that does not even exist yet.

So I believe I just have one or two more slides. Let me just highlight, I'm on loan from the University of Michigan to FDA for the calendar year, and there are five major priorities that I'm working on. One of them today is about fostering cybersecurity collaborations across the federal government, so I'm glad to be part of that community today.

Also, a big part of my role is training and mentoring, with respect to premarket and postmarket reviewing of medical device design as it relates to cybersecurity engineering. Because the best way to get a hold on these problems is to reduce the amount of I would say new legacy software that doesn't have appropriate cybersecurity engineering built in.

There's always going to be legacy software out there, and we will have to be spending quite a bit of time on post market as a result, but I believe it's really important that new devices entering the market have adequate cybersecurity controls so we can really tame this beast so the attacker stops winning so often. At that point I believe that's the last slide. I can end there and be glad to get back to the panel discussion with John. Thank you.

Denise Chrysler: Thank you so much to both of you. At this time, let's go to question and answer. And I'll just ask the first question. Based on an excellent question Jackie asked of our first panel, if you were in our seat, such as sending a letter to the Secretary of HHS with recommendations, what would be your two top recommendations to the secretary? And that was directed to each of you.

Kevin Fu: I have one piece of feedback to the secretary, and I believe this is representing FDA. I think it's really important that public health have a seat at the table when it comes to the newly designed cybersecurity safety review board that is being stood up by Biden's executive order.

This is essentially the cybersecurity equivalent to the NTSB, the National Transportation Safety Board that goes and investigates accidents, train and plane crashes. I really feel that public health needs a seat at that table, because public health is just so important when it comes to cybersecurity.

So I hope the secretary is able to find a way to include that, and certainly FDA is more than willing to help out in any respect there, because we care quite a bit about safety and effectiveness, and that board is going to be very key to everything we do.

John Guerriero: I would probably add to that, as Kevin was talking about in his presentation, just the different needs I think that the industry is looking to kind of develop when it comes to legacy systems, I think that is one area I think many different health and public health organizations across the country are really struggling with either upgrading or securing the different legacy systems that they are operating with within their own organization.

So I don't know if that would look at maybe increased funding to assist some of the different state and local organizations on doing controlled inventory of their different environments, and documenting

what operating systems they are using that are unsupported or maybe going to be unsupported, or that will be unsupported in the near future, and then updating or upgrading those.

And then probably the other part would be just on a high level really examining the information sharing of the different threats facing the industry and what are the risks that organizations face and how to mitigate that.

And I think some sort of streamlined part, maybe that is coming from the federal body, or if they would be working in tandem with other federal agencies such as CISA on working on collecting that threat information and then disseminating it out to the different local and state organizations.

And part of that might be really just strong encouragement for those organizations to join the different ISACs, the Information Sharing and Analysis Centers that are available to them. But those would be some of my recommendations.

Denise Chrysler: Those sound like great recommendations. Do we have other members of the committee? I'm trying to look for hands. John, I spent some time looking at the NGA's resource materials on cybersecurity, and there were a lot of materials there.

During our first panel, one of the first panelists recommended creation of playbooks, and she used some examples of preventing a security incident, and then a step-by-step playbook for responding to a ransom attack. Do you have recommendations on resources that already exist of that nature, either on NGA's website or elsewhere?

John Guerriero: Yes, that's a good question, because those are really, just even at a high level, some of those playbooks and guides on different how-tos, those are going to be tailored towards different audiences. So a lot of the work that we do will be tailored towards governors and their senior advisors, so we have done work on kind of collecting from different states, say what their statewide cyber disruption response plan looks like, what are the elements, what did they take from the federal model, how did they incorporate it and make it their own, and then what are some elements that might be, or the different models so to say, that other states can take and look and maybe use that to implement their own.

I would say CISA out of DHS is a really wonderful resource, they have a lot of different guidebooks. They've been really taking an active approach towards ransomware, they have a whole ransomware hub that has different playbooks, guides for things like that for private sector, for SLTT entities, as well as for I think they're looking to consolidate different recommendations for federal agencies as well.

But there's a lot of really good resources out there as well, outside of CISA, but as Kevin was mentioning NIST has a lot of really good, they're kind of all the different frameworks and recommendations that NIST compiled are really, they're probably one of the best compilations of everything that's out there in terms of what that environment looks like. They bring everything together, so it can get a little big sometimes.

But then other organizations sometimes look to take some of those recommendations and pare it down to say what a small business might be considering or what an SLTT entity may be looking at, like the

Center for Internet Security has what they call their top 18 controls, which are essentially different cyber controls that are based on the NIST framework but are a little more condensed for what would be actionable and implementable for a smaller organization. And then some of our partner organizations as well, like NASCIO, National Association of State Chief Information Officers, they have a really wonderful collection of different resources as well for state CIOs and state CISO, the Chief Information Security Officers.

I'm sure I'm failing to mention a few. Many of the different state partner associations will have different guidebooks and different playbooks for those. In NGA we did a governor's guide back in I want to say 2018-2019, and we're looking to update ours in 2021 or 2022 as well.

Denise Chrysler: Could you just mention what SLTT stands for?

John Guerriero: I'm sorry, state, local, tribal, and territorial organization.

Denise Chrysler: That's what I guessed, but I'm glad to have that clarified. We have a number of hands up, so let me go to Valerie.

Valerie Watzlaf: Thank you. I believe this question is for John, although I think we've heard this issue earlier this morning, and that's the talk about the shift to remote working, working from home, and how that could of course increase the risk.

So I was just wondering, are you hearing across the states that they're thinking about definitely bringing people back to the office, do you think then that that could actually lead to less cybersecurity risk, or anything that you're hearing in relation to that, particularly as COVID is lifting and so forth.

John Guerriero: That's a good question. The shift to remote work, not just, it was kind of a two-pronged part. It was the massive shift of just number of employees going to remove work, but also the rapid transition, where essentially it went in a number of weeks if not days where that was implemented, really put a strain on states and really increased the cybersecurity risk and the number of attack surfaces that were vulnerable.

But as the shift back, that's a good question, because many state employees have been back in the office, I think there will be some remnants of the risk posed, because one, I don't think the remote work is really going away, I think many states are considering, they really are looking at ways to increase the flexibility for their staff on remote work.

So a lot of those same policies and procedures that were implemented last March, they will kind of remain in effect. But I think a lot of the, one of the side effects of all that was really just kind of a raised level of awareness around the cybersecurity risks I think for your non-cyber state employee.

So I think a lot of states did a really good job of messaging out to their staff, there are increased cybersecurity risks when you are working remotely, the different procedures that staff were implementing, so like the VPNs, the different controls over personal devices, things like that, that maybe state employees may not have been as familiar with, now are increasingly more familiar with it. So there may be some residual effect of that as well.

I think probably the key thing about the cyber threat is that it's always changing, and it would be flexible and it's going to adapt to whatever the vulnerability is. So the vulnerability of last year is probably still in play, but it may not look quite like the vulnerability of 2022.

Valerie Watzlaf: Thank you.

Denise Chrysler: Let's go to Vickie.

Vickie Mays: Thank you for your presentations. I have a question for each of you. You kind of mentioned COVID. One of the things that COVID clearly taught us is about some small community practices and hospitals being very under-resourced.

So I'm wondering in terms of the state governor's level or something, if there's any assessment to know which of your clinics and hospitals, because they don't all have academic partners as we saw earlier, but the ability to identify and target individuals that need more help, and that are truly under-resourced.

And then the other is also to think about this kind of same notion when we start talking about medical devices, because as we look at again kind of small groups, rural hospitals, people are being sent home and needing to use wearables, needing to use lots of different things because they're so far away from the hospital that the care is being monitored using some of these devices.

Again, my question is we know these vulnerabilities exist, is there someone, some group that's responsible for identifying and suggesting fixes for those groups? Because for these groups, if something happens I think what we're going to see is a worse public trust issue. So I'd like to see if there's prevention activities in place.

John Guerriero: That's a great question. The latter half of your question, just about identifying and mitigating vulnerabilities, there are different assessment tools. Some states are looking to use different risk assessments, some states, and this is where it gets tricky, because if you've seen one state you've seen one state, and many states just have very different governing authorities when it comes to cybersecurity of different infrastructure, even when it comes to local government entities, and sometimes different state agencies.

But what there are, there are different assessment tools available, low cost, no cost, by the federal government. So CISA is another one, CISA has done a lot on the prevention side, one of their missions is to protect the cybersecurity of critical infrastructure.

So they do have different low cost and no cost risk assessments that are kind of easy to use, they have one aspect that is more of a kind of self-check or a self-assessment, and then they have more in-depth ones where a team will come out and they'll be on premise and they'll be actively searching for vulnerabilities within that entity's network.

That usually might be reserved more for a state network, but even then, I know sometimes the wait list for those services may take some time. And then the first part of your question was on how can states support local health care organizations?

Vickie Mays: Whether or not there are local healthcare, whether there are local entities or priorities that will ensure that small, rural, et cetera entities have what they need when there is a cybersecurity incident. The NIH just sent out an RFI talking about iCloud. I was a little stunned that iCloud resources in some of these poor hospitals and minority serving institutes apparently is something they're discussing in trying to determine what's needed. So I'm asking what is available to help them.

John Guerriero: So on the prevention and threat sharing side there is what's called an information sharing analysis center, and there is one specifically for healthcare. And so it would be free to join for all eligible entities, that would be any sort of public health or healthcare organization would be able to join, and they would receive alerts, they would receive different indicators or different threat alerts, different patterns of behavior, different techniques being used of kind of ongoing activity.

It would just be essentially allowing each one to know like this is kind of a threat, this is an alert, this is what's being seen over here, these are the techniques being observed, this is how to help prepare yourself against a similar attack.

Those ISACs also have a component where they are able to crowdsource different information from affected entities. And I know some of the different ISACs have a response component, although sometimes that would be much more in play with their state and local government partners as well as maybe the federal government.

Any sort of response would be likely internal or sourced out to a third party if the state does not actively support that response. It can be, this is kind of why one of the areas we focus in on is response planning, just because that can mean a lot of different things for states when it comes to federal capability, state capability, and then also the local capability, just what all of the different roles are there.

Kevin Fu: So to that question, through my role on medical device regulation, I'm not sure if I can speak to it directly since I'm not too aware of the resources available to the state and local, but what I can say is we really do at FDA depend upon coordination with state and local authorities when there is an incident involving cybersecurity.

I would say these information sharing networks, although they exist, they're still in their formative stages. And so we often have to rely upon quite a bit of informal communication in order to encourage local authorities to let us know what's going on when there's an incident, so we have to much more actively go out to solicit information.

And I would like to find a way, I'm not sure if it's because of lack of resources or just because it's a relatively new reporting information sharing structure, but I would like to find a way where state and local authorities will a little more instinctively know oh, if it's involving a hospital on the OT, the operational technology side, they ought to include FDA, at least keeping us in the loop, in case we may know some things that are more at a national level that we might not pick up on if the state and local aren't sending in effectively signals of potential problems that could be come in.

Vickie Mays: Thank you.

Denise Chrysler: Nick?

Nick Coussoule: This question is directed to Kevin. I think you talked a little bit earlier about the engineering principles that have been around for quite some time, in regard to designing products. My question is a little different. I think it's pretty straightforward, obviously if you're building something new or something from scratch, but whether it's a product or other things that could be potentially compromised by security, are there any of those principles that you believe are most relevant for dealing with existing kind of ecosystem of either products or capabilities that then could potentially be leveraged in either communication or recommendation models through HHS or other entities?

Kevin Fu: So your question is basically which principle would be most helpful for the pragmatic reality of their legacy systems out there, is that effectively what you're asking? I think one of the principles that can be helpful there is a notion of sort of short-term versus long-term remediation.

One of the principles that's known as the least common mechanism, it's basically the idea that you avoid mixing different systems together too much. And so the analogy sometimes I like to use is you don't store your lunch with the crown jewels, because obviously if you're getting your lunch every day you're likely to lose the crown jewels.

Knowing that a particular device has intrinsic fundamental vulnerabilities will change your risk management strategy. So you might treat I almost like effectively the cyber equivalent to hazardous waste. You wouldn't be going around with tainted samples just touching everything, if you've got a device that has some known problems, I think you need to be a little more mindful about what you're connecting it to.

A challenge of course is going to be a lot of the connections that happen between computers and medical devices are unintentional. There are obviously intentional connections, say you want to connect it to an electronic medical record system, but then there's accidental ones. Vendors will sometimes have cellular modems built into their legacy devices to call back to the mothership, and sometimes HTOs don't even know there's a cellular modem on the inside.

So it can be difficult in practice to isolate, but isolation, I wouldn't say it's a great approach but it's one of the only approaches to reduce the risk. The problem with isolation is it has an ungraceful failure mode. So when that isolation is pierced sort of all bets are off. So that's why I like to say the firewall approach, yes, use firewalls, but if you're relying on firewalls as your singular protection mechanism, when that firewall fails, again all bets are off.

So the key is to find graceful failure modes for those legacy systems. One other non-technical approach that is a subject to debate today is the notion of end of liability. The idea that at what point does old software become a liability of a different entity, when does it shift from the manufacturer to the HTO.

I would say today there's probably quite a bit of contract language where it's unclear who owns that liability, and there will likely be finger pointing as a result. So I think more clarity at the procurement level can be more helpful in removing some of these economic externalities of who owns the risk. I know that's not a complete answer, but hopefully that gives you some idea of my thinking.

Nick Coussoule: The only follow-up I would have to that a little bit is the question of who owns the risk is a very interesting one when you start talking about third party reliability. I think we'll probably get into that in a different discussion, so I'll leave that one alone for right now, but thank you.

Denise Chrysler: I don't know if this fits in, I've been thinking about procurement process. I was a state attorney for 27 years, and when my agency would send me contracts involving any sort of technology it was like, and of course you're looking at the different provisions about risk and liability and all that sort of thing.

I was just thinking about, assuming that government is updating its antiquated systems or its homegrown systems, and this would be both for the public and private sector, when you're contracting vendors do you have recommendations, this could be Kevin or John, on how an organization might be proactive in addressing security risk in the procurement and contracting process.

Kevin Fu: There are a number of groups working on different ways, sort of playbooks for procurement from the HTO perspective. I would say this probably started mostly with the Mayo Clinic almost ten years ago, they called it their Vendor Book, and they would share it with anybody who asked, and it was sort of tips on what you put into procurement language when a hospital is buying a medical device, with respect to computer security and post market maintenance of all the software updates and operating systems, security updates.

Today there's quite a bit of an active community within the health sector coordinating council as it relates to procurement. I wouldn't say it's a done deal, but that's where I would point people to go, the health sector coordinating council for that community. I'm sure there are more that I might not be aware of.

John Guerriero: To add on to Kevin's piece, procurement is a huge cybersecurity risk for states, not just in the healthcare sector, but all across the board. Really supply chain risk has been across the headlines a bit as well. What we've been seeing, especially with local organizations, so maybe that's the local healthcare organization, the local county healthcare organization, or maybe it's the local government.

So one, they rely on third party to do a lot of cybersecurity functions. They might not have a full-time dedicated IT staff, so they really do rely on those third-party contracts, third party vendors. And they may not just be as familiar with what to ask during that process as Kevin mentioned, just having some sort of guide or resource available that puts into non-technical terms for some of these non-technical staff to ask vendors, and to make sure they're in different contracts.

And then also clarifying expectations, what would be the role of the third-party provider or the vendor in the event of some sort of incident, what are the different regulations around response. Those would probably be top of mind. And then just thinking through as well, I think just putting it into the non-technical piece I think that's essential too for many of the smaller organizations.

Denise Chrysler: Let's go to Jacki.

Jacki Monson: This question is probably for both of you. I want to poke a little more on the legacy system. I think John mentioned as something that we want to solve. So this is a prominent issue,

particularly in the biomed space, and both from an operating systems standpoint as well as just the mere fact that we have really expensive biomed devices.

I personally don't think it matters what's in a contract with respect to our legacy problem, because it's a legacy problem that continues to carry on because we're still using these biomed devices, and they have security vulnerabilities and opportunities.

And so I'm curious what your thoughts are. I can't imagine an incentive program for let's say a radiology imaging machine that's $200,000 being something that's realistic to incentivize all of healthcare to phase out that old technology that doesn't have the good security controls that that brand new radiology imaging machine has today. So what are your thoughts on that sort of area around the legacy technology and what potential recommendations you have to solve it?

Kevin Fu: I don't have a silver bullet for the legacy systems out there, but maybe let me talk about the where I'd like to see things go, the way I view legacy. I view everything as legacy. The moment a device gets approved or cleared it's already legacy, it's already running on an outdated operating system. And so the real question to me is twofold: is it secure to begin with, and is it securable for its intended lifetime.

For instance, if you ship something with Microsoft Windows Microsoft tells you the day you install it the day that they're going to stop providing updates. So that's a known, completely known, there's no mystery there. So the idea that a device depending on it could last longer than that deadline, I don't understand that argument. So that cuts to make sure it's secure when it's shipped, make sure it's securable and patchable.

In fact, FDA has a published fact sheet dispelling myths about security in medical devices, where we say we expect medical device manufacturers to provide regular software updates, full stop. They're expected to, to keep things safe and effective. But with regards to what do you do with all the legacy stuff out there, I would agree it's a huge problem. And I would argue it's even worse.

So I know internationally, what happens when a hospital wants to try to get a little bit of the residual value out of their old MRIs? You sell it to a foreign country. I'm aware of foreign countries using just extremely antiquated medical devices. And I'm aware of one that even had to circumvent some of the security controls because somebody stole their USB stick with their license key. Just very strange subcultures reprocessed medical devices, outside of FDA's purview.

John Guerriero: From my perspective it's probably less technical on the healthcare side, but more concerned with just the legacy systems that are just abundant all over state and local government. The networks, the software, the hardware that are being used are sometimes very out of date, and just the funding to upgrade is just not available.

And from the state and local government perspective that's a huge obstacle when many of the threats you are facing are coming from very advanced, malicious actors, sometimes nation state actors, and in our work we see this a lot on the IT systems and in the election infrastructure side, but I think the case is very similar probably with healthcare as well, where there just needs to be more dedicated funding for state and local governments to upgrade and update their systems.

And I know NGA has been in the past advocating for increased or established grant program for state and local territorial and tribal governments to have some sort of cybersecurity grant program where they can use additional federal funding for those areas, or for legacy upgrades, because I agree with Kevin 100 percent, that is probably one of the top if not, it's probably top three if not top concern facing state and locals when it comes to cybersecurity.

Denise Chrysler: Let's go to Melissa.

Melissa Goldstein: Thank you. I have two quick questions for Kevin. Kevin, when you first started speaking today, you mentioned that maybe way back in (audio problem) your primary concern was about (audio problems)

Denise Chrysler: It seemed like you were losing connectivity.

Melissa Goldstein: Sorry about that. Kevin, did you get the first question about your predictions, in response to your statement that in 2008 your primary concern was ransomware coming down, I'm interested in your predictions for your most primary concern five years, ten years, what should we be thinking about now. The second question is your statement of the importance of public health being at the table as we develop the new advisory group for the cybersecurity, the executive order.

And I'm wondering if you mean public health to the exclusion of medical organizations, healthcare organizations, clinical care, or if you mean both, do you mean public health kind of like CDC public health, that's what I'm interested in.

Kevin Fu: Why don't I answer that second one first, because I think that will be the shorter answer. When I say public health at the table, I don't mean as displacing another group, and I mean it even more generically, because the executive order doesn't even mention HHS at all in it by name, it mentions federal civilian executive branch agencies. And so the phrase public health doesn't even appear.

So I don't mean anything particularly specific, other than I sure hope public health will be represented, since it has some unique constraints as we're discussing today, that are going to be different from say automobiles or internet lightbulbs, where I think it will be important to have subject matter experts in public health in cybersecurity.

For your first question, I think that's much more nuanced. So first of all, let me just correct my statement. So when I was referring to ransomware, I wasn't predicting ransomware, and I wasn't saying ransomware would be a problem. But what I was predicting was that the unavailability of healthcare would become a big problem.

Because to me, and I'll have to preface this with big parentheses, in my role as a professor in presenting that ten years ago my biggest concern was that breaking into medical devices seemed about as easy as breaking down an open door. Because at the time there were no sort of coherent standards on this topic.

So of course, you're going to have legacy systems with problems. Even if you meet the requirements, of course there are going to be problems, because many of the advances on medical device security hadn't been done yet with regulatory guidance.

So my big concern was garden variety malware could break into a hospital without very much intention at all, simply because it's an opportunity, and then cause systems to go down. I didn't realize that would take the form of ransomware, but it sure has. So that's still a concern today.

Now, with respect to your question about what about five and ten years from now, what are you going to be talking about, perhaps in this committee, I predict it's going to be about the sensors inside healthcare devices, whether it be medical devices or general wellness.

I'm a little less concerned about step counters, because the safety implications, they're not automatically dosing medication as a result. But anything therapeutic or diagnostic that's making an automated decision without a human in the loop based upon a sensor, that to me is going to be a five-to-ten-year problem.

Once ransomware is solved that's probably going to be the next big problem that's very attractive to monetization from the criminal enterprises for cybersecurity. And let me just clarify by the sensors. You can manipulate a sensor into delivering false information which can then cause the algorithms to do untoward things with diagnoses and therapy.

Denise Chrysler: John, I've sort of lost track, I can't remember who went first.

Rebecca Hines: I think those questions were just for Kevin.

Denise Chrysler: Maya?

Maya Bernstein: If there are no other members that have question. I will defer always to the members first. I did want to follow up what Melissa was asking Kevin, which is given some of the testimony that we heard this morning, that based on your predictions about what the next thing is in five to ten years that you're concerned about, medical devices and sensors and so forth, but also thinking about what we heard about ransomware, that it's not just the threat of unavailability of information, but that our attackers are now extorting information and threatening to disclose information or use information in improper ways, what are you thinking about what FDA might do about that?

Traditionally FDA has not considered the leakage or the use of the information associated with a device as a threat or as a health safety issue, it hasn't considered that a threat in the past, but given that now seems to be where this is going, and that medical device manufacturers are not covered by HIPAA, do you think that FDA may extend the way it's thinking about the safety of devices to also include privacy of information that might leak out of devices?

Kevin Fu: That's a good question. It sort of depends on what hat I'm wearing. But representing FDA at the moment, our congressional remit is only for safety and effectiveness. So there would have to be a strong argument connecting the privacy to a safety or efficacy issue. The only argument I'm aware of at the moment, and certainly educate me if you know of others, would be for psychological harm.

So there are certain extremely sensitive things like HIV test results where if there's a privacy problem that could be considered patient harm. But I would say it's very context sensitive. So I can't obviously speak for other agencies within HHS, but I know privacy is spread across different agencies within the department.

Maya Bernstein: Certainly, in the privacy world we think of other kinds of harms rather than to medical safety, we think of harms to reputation or embarrassment or things like that, or even financial harms that may come from the disclosure of information, discrimination and so forth, which are not the traditional things that FDA normally thinks about. So if we wanted to protect those things, I mean, given that those things may happen as a result of compromise of medical devices, do you think FDA is in the best position to do that, or FTC, or some other entity, to look at those kinds of problems?

Kevin Fu: I think FDA will always have as its core area of expertise safety and efficacy. And I think there will certainly be challenges, I'm not saying it's impossible, but I think there will always be challenges if it's a little bit off mission from the congressional remit, unless Congress decides to assign a remit –

Maya Bernstein: We could seek authority to do that, seeing a problem for example, one could seek authority to do that. Nobody has the authority to look at medical devices right now is the point, in the kind of harms that I'm talking about.

And so is it, I guess what I'm asking for is who do you think might he in the best position to work on those kinds of problems, is it FDA because their expertise is in the devices, or is it OCR because of their traditional civil rights or HIPAA, or is it FTC as a consumer protection agency, do you have any thoughts about that?

Kevin Fu: My thoughts are going to be its' going to take a village, and you're not going to find any one agency I think that's going to be sort of already stood up to say hey, we're perfectly suited to handle this. But you're going to find elements of it in different agencies. So FTC, obviously has quite a bit of experience. I would characterize them as post-market, since it's mostly through the court system. So that's not going to help. Where FDA tends to do a lot of effort on pre-market, we're one of the rare groups where a manufacturer has to come to FDA for effectively permission to sell a medical device, whereas FTC would be after it's sold.

So I would argue that there's probably an opportunity for some kind of workshop or melding of the minds to get experts from different agencies to come together to sort of do a SWOT analysis, what are the gaps, what do we need to know. A little bit less about what we're doing and more about what we could be doing.

I also think there are lessons that could be learned from the evolution at FDA, because if you look back 15 years ago at FDA it was a very different agency with respect to computer security. Forget privacy, even security, it was considered like well what does that have to do with safety.

Today it's a completely different ball game at FDA, it's clear that you need to have reasonable cybersecurity to be safe and effective. I think there can be lessons learned from how agencies evolve, even when the remits remain relatively the same from Congress.

Maya Bernstein: Thanks, that's very thoughtful.

Denise Chrysler: Thank you everybody. I appreciate, I want to on behalf of the committee express our appreciation to both of you for your valuable input. I know my mind is whirling. And especially thinking a lot about role-based access, which I'd always under the HIPAA privacy rule thought of as a privacy issue, but now really recognizing its relationship to security and so many other issues that you have raised here today. With that let's move to panel three.

Panel III — Emerging Security Threats and Preparedness Across the Healthcare Industry

Nick Coussoule: Thank you, Denise. So I'm here to help moderate our third panel, which is entitled Emerging Security Threats and Preparedness Across the Healthcare Industry. As we've demonstrated in the earlier panels today, security and healthcare are a quite interconnected and evolving subject.

The transition from a primarily paper based to a critically digitally based operating model has advanced healthcare capabilities but created opportunities for significantly elevated risk and exposure, both from a frequency perspective as well as a scale perspective. Our next panel topic as I said is emergency threats and preparedness. Hopefully we'll cover some of the historical trends as well as some of the new challenges that are coming up.

We've got two excellent presenters here. I will introduce them both briefly and then we'll let them highlight a little bit of themselves as well as go through their prepared remarks, and then open it up to questions from all the panelists.

Our first presenter is going to be Suzanne Widup, she is a Senior Analyst at Verizon Enterprise Solutions, coauthor of the Verizon Data Breach Investigations report and lead author for the Verizon Data Breach PI report. So I think we'll get a good overview of that coming up in the session.

But she has a lot of background not just as an author but actually within the technology realm as a systems administrator, security engineer, digital forensics, in very large environments. She has a BS in computer systems and a master's in information assurance, so I think she'll be an excellent topic for us to be able to cover.

Our second speaker is going to be Kevin Stine, he's a Chief of Applied Cybersecurity Division at NIST, the National Institute of Standards and Information Technology Laboratory, but in that role he's the acting Chief Cybersecurity Advisor and Associate Director at NIST Information Technology Laboratory.

Again, leads the collaboration with industry, academia and government to improve cybersecurity and privacy risk management. I think as funny as Denise was just talking about the tie-in between privacy and security, it's really pretty intense at this point in time and it's really difficult to separate those topics. And then a lot of collaboration and application of standards.

So without further ado I will let them highlight a little bit more of their backgrounds before their presentations. But we'll start with Suzanne.

Suzanne Widup: I am Suzanne Widup and I am here to talk about the research that my company produces annually, the Data Breach Investigations Report or DBIR for short. I've also pooled data specific to the healthcare industry for this session. Now if you're not familiar with our research, this is our 14th year of publication, so we've been doing it for quite some time, and I have been one of the coauthors for the past nine years. This is not based on a survey, so this is much more rigorous than that.

For each of the cases that are worked by our own forensic practice and by our partners, the facts of the case are gleaned and recorded, and then once we do that with all of them, and you'll see we go through quite a few security incidents to boil down our research, then we basically run our reports and write the report based on what the data is actually telling us. So this is our basic demographic slide for the report this year.

We had 88 countries represented in the data this year, 83 contributing organizations. You can see we went through almost 80,000 security incidents to boil down into the just over 5250 confirmed data breaches. Now, to be a confirmed data breach in our dataset it actually has to be a confirmed compromise of the confidentiality aspect of the data, not just potential exposure.

And so the classic scenario where you have a stolen laptop, you can't actually confirm that the data was accessed on the laptop because you no longer have custody of it and you can't do forensics on it, and so that would be considered a security incident in our dataset and not a confirmed data breach. So when you look at our numbers keep in mind that this is potentially just the tip of the iceberg, the problem is possibly considerably larger.

So the combination of login and password is very attractive to the attackers. These basically allow them to masquerade as a legitimate employee and make it much more difficult for the people defending to detect that they have been compromised. Over the years there have been a large number of very large credential breeches that have then been posted in public forums for hackers to gather up together and build their own datasets of these kinds of (audio problem)

Nick Coussoule: Suzanne, we can't hear you. We lost you about a minute ago.

Suzanne Widup: Sorry about that. Occasionally my headset likes to disconnect without telling me. So basically, the combination of login and password is what we're calling credentials, and it is very much a target of the attackers because it allows them to masquerade as legitimate users in your environment, which makes it much more difficult to detect them.

There have been very large credential breaches over the past several years, and they have been posted on public forums for the attackers to be able to compile their own datasets of these kinds of credentials, and basically use them against any infrastructure they can access.

So if you have employees that have used their credentials, like the identical login and password in multiple places, if you think about it so many places allow your login to be your email address, and so that's half of it right there.

If they're reusing their passwords, it means that these will have a certain amount of success wherever they've tried them, and so that speaks to the need to deploy some kind of control like multifactor

authentication to make these kinds of breaches less valuable to the attackers and yourselves of course less vulnerable to these kinds of attacks.

So there has been talk by previous presenters about the ransomware problem and about the change of tactics where they are grabbing a copy of the data prior to triggering encryption to use the threat of an actual data breach as leverage to make their people pay up. It used to be that it was just ransomware attacks were not considered data breaches because of course they didn't do that, they just made it unavailable. But since they have changed their tactics, it has become 10 percent of our breaches in our dataset for the past year's report, and that was quite a change.

So we are seeing with this past year's dataset that the cloud assets are being attacked more often than the on premises, as people in the pandemic moved to the cloud so did the attackers. It may be simply that it's a matter of them being more accessible when they're in the cloud than when they are on premises, but either way we are seeing considerably more than we did before of cloud assets being attacked.

Now one caveat here is we don't always know where the asset that was attacked was located, whether it was on prem or in the cloud, and that's a big enough percentage that it might tip it either way if we did know. But so far it's looking like cloud is a significant vector.

So this is probably not a surprise to most people, that the people who are attacking you do not work for your organization or for your partners, and that they are motivated by money. So criminals will follow the money wherever it goes, we can count on them for that.

And we did see a decrease though in the internal actor breaches. Now the one thing about internal actor breaches is you do have to understand that it's not just malicious actions, it also includes the error action. And so it's interesting that they are going down proportionally, but there's always going to be more people that don't work for your organization than who do, so it would make some sense.

So this is the data that I've pulled for this session. We have cases that are waiting to be coded in what we call our public dataset. So what we're doing with that is we are taking publicly disclosed data breach notifications from the news, from HHS, from all kinds of places, and we use that to augment the data that is sent to us by our partners annually.

And so this is something that I could pull now, because we haven't started data collection for next year's report, so we don't have anything from our partners yet. But this is the actions and how they broke down for starting in November 1st of last year to present. And you can see that hacking and malware are a huge problem, and errors as well as the misuse action, which is people doing malicious things that work for you.

One of the things I thought was interesting here was the tactic change in the malware, the ransomware actors, represented 25 percent of the ransomware cases that were there last year. So that's, it's now 25 percent of these cases that involved malware involve ransomware and involve them taking a copy of your data.

The other interesting point in the data was that five percent of these were actually attacks on the business associate, not on the organization that had to do the notification. And it really sort of illustrates the increase of supply chain as a vector of attack. And so when you're taking on business associates of any description, any vulnerabilities they have are vulnerabilities you now have. And I think that's something that tends to be sort of skipped over in a lot of the contracts and risk assessment that people do.

So we have attack patterns to discuss. If you're not familiar with our research, in 2014 we did a cluster analysis of over 100,000 security incidents, and we came up with nine attack patterns. And we really did that because it's easier to get your arms around defending against nine attack patterns than it is to figure out how to defend against the 100,000 security attacks.

This is the data which we updated this year. We updated our patterns, and this is how it played out for breaches and incidents in the dataset. And in the actual report we actually do mappings to controls that will combat both of these kinds of security incidents and breaches, to sort of give you an idea of where to go from where you are.

So this graphic shows our patterns over time. You can see the rise of the social engineering attack which drove our reevaluation of our patterns this year. And you can also see the top four here are the basic web application attacks, social engineering, miscellaneous errors, and system intrusion. And those with the exception of the social engineering were very much prevalent in the healthcare data as well.

The one thing that you can see here really decreasing was the lost and stolen assets. This was very much a problem in healthcare for a very long time and has largely been eradicated by implementing encryption on the mobile devices so that when the device goes missing the data is still not at risk, and that's been a huge thing for healthcare, because it took a very long time for that to go down.

The basic web application attacks, if you look back at the slide, I had with all of the hacking, this is where most of those fell. These are very simple attacks, they tend to be either brute force of the credentials or they are the use of the credential stuffing, when they have all those compiled credential breaches and they're just using them against your infrastructure. And so that's where a lot of those fell. And you can see here the prevalence of the cloud versus the on premises as well, and it's really just a matter of it being easy to get to I think.

This one really is showing the problem of the credential stuffing attacks. So we had data here that shows that some organizations had just 637 attacks over a year. Others had 3.3 billion attacks thrown at them over a year. And these are just credential stuffing. These are people throwing known credentials that have been breached at your infrastructure and seeing if any of them actually get them in.

So the system intrusion pattern is where the more complex attacks fell. So this is multistep attacks, they will use multiple actions such as hacking and malware or social to start an attack and then progress through. So they're sort of working harder for these attacks than they are for the one we just saw with the basic web application attacks.

And this is where most of the ransomware and the other kinds of malware found their home. It was interesting to see sort of the complexity increase as they went into this. We sort of think of this as the smarter, older sibling to the basic web application attack pattern.

Miscellaneous errors. So this is a big problem in healthcare, looking at which roles are the most prevalent here, you can see that they are the ones that are most likely to have increased access to data as well, the system administrators of the world, the developers, they're going to have a lot of data that they can pull. And the scenario that we've seen time and again here has been the system administration person stands up some kind of data store on some cloud infrastructure without the kinds of controls that you would normally want to have on your data.

And then you have the combination of that and the next slide, where they are found by a security researcher. So these are people who have specialized search engines like Shodan where they're looking for these kinds of data stores that have been put up on the internet without their controls in place.

And so they will find them, they will make some kind of determination of who owns the data, and then they will make a notification to the organization. After that they will most likely notify the media. Now, you get a lot of people don't like the security researchers because of course they're doing this in part for their own advancement and notoriety.

However, as someone whose data has been compromised many times, I would far rather someone who is going to make the notification to the organization and hopefully get the data taken down be the one who finds it than your average hacker who is going to take a copy of it and sell it to six of his friends. And so it is something of shooting the messenger, and yet the data is still out there whether they find it or not. So I think it's still better they find it than someone else.

So the privilege misuse pattern has been a common problem in healthcare as well, for some time. This is the malicious insider, and they're using the access that they have been granted to do their job to do something they shouldn't be doing, whether it is snooping on the data, which occasionally does happen, or it is actually using the access they've been granted to steal the data and either try and monetize it themselves or sell it to someone who can monetize it easier. And it has been a problem, it's going down, but it really is something that tends to happen a lot in healthcare as opposed to some of the other industries.

The other thing that we see with these kinds of insider cases is they take longer than average to detect. And in reality, most of our controls tend to be facing the outward perimeter, looking to catch someone from the outside coming in, and it really illustrates the need to also be able to detect when someone is misusing their access and looking at data they shouldn't be for whatever reason.

So we break our data down in multiple ways in the report. One of those is by industry. To do that we use the North American Industry Classification System or NAICS codes, and you can see them here, those are the numbers that are next to the industry names on the bottom of the columns here. So what we do here is we break this down this way to show the readers that different industries really are experiencing breaches in different ways.

And the other thing that we do, I don't have a graphic here, but we have it in the report, is we also map the industry and the patterns here to the Center for Internet Security Critical Security Controls. We use implementation groups one, two, and three, so we map to all of them.

And if you're not familiar with those it's really good to use as a roadmap. So if you are in healthcare you see what you're most likely to be hit with as far as the attack patterns go, and then it gives you a roadmap, if you're just beginning in your security journey, this is the kinds of things you should be using to combat that kind of attack.

And then as your security maturity grows over time you can start looking at the other implementation groups, and they build upon each other. So it's quite useful that way as a roadmap for getting your ducks in a row so to speak security wise.

This is our healthcare slide from the report, the section on healthcare of course is a little more robust than this slide shows you. But basically, the top patterns this past year were miscellaneous errors, basic web application attacks, and system intrusion. And here you're seeing the breakdown of what the varieties in error are. Mis-delivery is just simply when you send something to the wrong person, whether it's through email or very commonly via mass mailings when the envelopes and the contents get out of sync. Publishing error is when you publish something that should be private to public facing systems.

And of course, misconfiguration is those databases typically that are stood up without any controls. We do find that miscellaneous error was the top in the dataset that I pulled for this coming year as well. So as long as the data that our partners contribute is in line with that, which it probably will be, it's still alive and well in healthcare.

So hopefully this has been helpful. We do encourage you to read the report. You can download it from the link there. I think they may also have it available for you here. And then you may also be interested in the VERIS Community Database Dataset, which the ones that I pulled for this session have not been coded yet, they won't be coded until we start data collection in November, but they will eventually also make it into the dataset.

And we can have the last slide. This is information if you want to be able to contact me. And then the last @VERISDB is a Twitter handle for a data breach feed as I find data for the public dataset, I tweet it out. So this is basically a live feed for data breaches that are current.

Nick Coussoule: Suzanne, thank you very much. Although I'm not sure I want to say thank you for sharing that with us, as it's both I think it's really good information, a little disturbing. But thank you very much for sharing that with us. We'll now turn it over to Kevin please.

Kevin Stine: Thank you for the invite to talk with you all today. I think I've met many of you over the years, so I appreciate the opportunity to come chat with you today. I am Kevin Stine, I do work at NIST, National Institute of Standards and Technology. I wear a number of different hats that Nick described earlier.

What I'd like to do today, and again I want to thank not only this group but also we have longstanding relationship with many different parts of HHS, very strong relationships, close collaborations, and it has always been very productive and exciting relationship to have over many years, not the least of which OCR, Office of National Coordinator, and the FDA for sure.

Actually, before I started at NIST a little over 14 years ago, I guess I actually was at FDA for about four years, more on kind of the operational CIO shop side, as their first at the time, Chief Information Security Officer. It was an interesting time to start both my federal career as well as federal cybersecurity at that time. I started, and then two months later the Federal Information Security Management Act was passed, which certainly a lot has evolved since that time, both on the legislative front as well as on the threat environment and the technology landscape as well.

So I enjoyed my time at FDA, and that allowed me to pivot over to NIST, where I started my work here mainly in the healthcare cybersecurity space, and then I've grown and broadened over the years.

So I thought what I would do today, I just want to do a quick level set on NIST and what we do from a cybersecurity perspective, and then touch on a handful of current areas where we're focusing on, I think the scary trends and patterns that Suzanne mentioned I view in some ways our role as helping to produce in collaboration with the community the standards guide to many of the resources that can be helpful to better manage those types of issues, in a variety of different contexts.

So real briefly about NIST. Ultimately NIST is a nonregulatory agency, part of the US Department of Commerce, and our mission broadly focuses on standards and measurement, and a lot of different technology domains and innovation domains. More specifically from a cybersecurity and a privacy perspective, and I appreciate the questions previously on privacy, that's an area we continue to increase our emphasis on, from a security and a privacy perspective we really seek to cultivate trust in technology, and we try to do that through advances in standards and technology and measurement science.

I really think about our work spanning this lifecycle if you will, from the very early stage, fundamental research, into the potential application of that research in a variety of different contexts, and using that to then inform the development of standards and guides and other practices, but ultimately leading to how do we help organizations to practically apply, practically adopt and use those in ways that will help them better manage cybersecurity and privacy risks in the context of their missions and their business objectives.

So our work spans this entire thread pulled from left to right depending on which way the camera is facing right now along the way. Cultivating trust, back to our purpose if you will, cultivating trust is not just the trust in the resources we produce, it's just as much in the process we use to produce them. So everything we do is done in a very open and transparent and collaborative way.

We want to leverage the experiences and the expertise of individuals and organizations all around the world, both on the technology side as well as on the mission or business process side as well, so really tapping into the experience of those practitioners is key, and such a critical tenant of our work. I think a

lot of the resources that we produce collaboratively are intended to help address and manage risk from many of the patterns and the trends that Suzanne discussed earlier.

So I'm going to cherry-pick just a handful of relative initiatives or resources that I thought would be helpful for this discussion as I listened to some of the previous panel with Kevin and John, and then hearing Suzanne and some of the questions, I believe there are some others that we'll talk about when we get into the Q&A.

So first we do have a foundational healthcare guide, it has a particular focus on the HIPAA Security Rule and helping organizations to implement that. We last updated that quite a while ago, back in 2008 I believe, October 2008. Certainly, a lot has changed with respect to cybersecurity and healthcare, and cybersecurity broadly, technology trends broadly. Many of our own resources at NIST and resources developed by HHS and others in the community have evolved as well. So we're long overdue for an update to this.

A couple of months ago we put out what we call a pre-draft call for comments to get feedback from the community, given all the change and all the evolutions in this space, with respect to the HIPAA Security Rule and really the broader healthcare and cybersecurity domain, what are some things we should be considering as we go about an update.

And we got a lot of feedback, it was tremendously helpful, and we're in the process of adjudicating that right now internally so that we can then produce and issue an updated draft guideline for public comment, really with the objective of helping to educate readers about the HIPAA security role and the cybersecurity terms and capabilities in the rule, again working with OCR on this, amplifying awareness of NIST and non-NIST resources that are relevant to helping an organization better understand how to implement those capabilities within the context of the HIPAA security rule, not just for the covered entities but certainly for the business associates, and really any individual or entity in the healthcare space. So that pre-draft call for comments just closed just a handful of days ago, I think it was last Friday, and we're poring through that now. So more to come on that as we get a little further down the process.

It's one thing to produce the documentary resources, the guidelines. But I think if you remember back to that life cycle thread that I talked about with respect to our different efforts, on that far right or far left depending on which direction you're looking at a slide, you have really getting down to practical application, how do we help organizations take the standards, take the guides, take existing technologies that exist today and apply those in ways that will help solve specific challenges that their organizations may face.

And that's really the focus of our national cybersecurity center of excellence, which was stood up in 2012-2013 timeframe thanks to the hard work of then-Senator Mikulski, at the time the Senior Senator from Maryland. Really thing of the NCCOE or the Center as an applied cybersecurity lab. So how do we accelerate the adoption of secured technologies.

And we do this by working with stakeholder communities, and those could be stakeholders focused on broadly applicable technology platforms such as cloud or mobile devices, mobile technologies for

example, or sector specific interests such as work with the healthcare sector, and even subdividing that down potentially further depending on the challenge.

We work with the community to identify very specific and tightly scoped cybersecurity challenges that are affecting their business operations. In the case of healthcare, things that could be affecting their ability to deliver better care because of a cybersecurity challenge or concern that they have.

And as we define those problems at the Center, we then roll up our sleeves with industry, the folks that have produced commercially available technologies to help build out example implementation, so not giving the answer, but one answer, think of them as blueprints, for how you can take those existing technologies, existing standards and practices, and integrate them in such a way to prove out an example solution. We do work with real products and technologies, we work with the companies, we issue those architectures and essentially everything including any kind of glue code that we had to use to make those architectures real, and we build those out using the real technologies.

On the left is kind of the current collection of healthcare specific resources, certainly if you're not familiar with these I encourage you to take a look at them, and for a few of them, I certainly have one listed there, there's a short video that talks through what we've done on the securing wireless infusion pumps work, which was a very fascinating project. I can certainly get into more detail if you like.

Suzanne talked quite a bit about ransomware and some other issues, and certainly ransomware is top of mind for everyone these days, so much so in fact that we actually are hosting a workshop as we speak through the NCCOE at NIST on ransomware, preventing and recovering from ransomware and other destructive cyber events. This was running from 11:00 to 3:00 today, just a mini virtual workshop, I think we're all getting virtual workshopped out, so we try to keep it concise and hard hitting. That's actually happening today, that is being recorded so it will be available.

But the intent of this workshop today is to better understand the challenges with respect to implementations, operations, and security regarding ransomware, whether it's on the prevention or protections side as well as the response and recovery side. Identify what the existing standards and practices are that are available and what are some of those gap areas in technology space as well, with an eye toward helping organizations to improve their ability to protect against these attacks, and then respond and recover if they do happen. I think I mentioned we do have a workshop today that will be made available, so you can go back and watch that at your leisure.

Certainly we have, and many of you are probably familiar with the cybersecurity framework that was issued back in 2014 and updated once since then, and continues to see broad adoption, not just domestically in the different sectors but globally. That's a great tool that can be customized in the context of different sectors and different business operations, but also in the context of different threats.

So we've issued what we call a preliminary draft profile for ransomware risk management, and part of the workshop today is to get feedback on that so that we can refine that as a much more usable, digestible, and practical tool to help organizations understand steps they can take and approaches they

can implement to help them across that protection, detection, response and recovery side of ransomware activities.

There's been a little bit of talk already today on third party risk management. This is an area that we have a longstanding interest in, in the broader supply chain risk management space, certainly in the cyber supply chain. Think information and communications and operational technology, so the IT, the OT, and kind of the different points of intersection between those two.

Users of those technologies really rely on complex and globally distributed and interconnected supply chains, and I think there's a lot of different entities at multiple tiers of outsourcing and diverse distribution roles and those types of things within the supply chains that we're all operating in and leveraging today.

Our efforts are really focused on helping organizations to manage the increasing risk of cyber supply chain compromise, whether those are intentional or unintentional. We do have some foundational guidance that's in the midst of an update right now.

If you track the NIST number it's SP or Special Publication 800-161, Cyber Supply Chain Risk Management Practices for Systems and Organizations. So we always appreciate comments to help inform that. We're also trying to take, and we have received a lot of comments on that, I think those comments were received in the last couple of weeks, I think that closed at the end of June.

So we anticipate releasing a second draft of that resource probably late summer early fall, thinking the September-October timeframe. And then a final version probably sometime in the spring next year.

We're especially interested in feedback from organizations on whether the document provides the guidance and structure that any organization can use regardless of their size or their mission, or their sector for example, and whether it's sufficiently descriptive to be clear and actionable. Again, we have this increasing emphasis on clear and actionable resources. So things that organizations can take today and use in meaningful ways.

I'm sure you're familiar with an executive order that was issued about two months ago, I think two months ago yesterday or two days ago, EO 14028 on improving the nation's cybersecurity. Here is a little timeline of the NIST-led activities as a result of the executive order. We're partway through that.

Our focus in the EO, the things we were directed to do, were really focused on enhancing the software supply chain security. So our early-stage activities are really building on existing guidance around software security, supply chain security, and kind of the points of intersection there. Latter stages on this timeline are really where we're going to revise, enhance, or create new resources to help in response to the EO, again with an eye towards practical and actionable.

I do think beyond software supply chain security, other parts of the executive order really highlight things like zero trust and secure cloud migrations and multifactor authentication and encryption of data at rest and in transit, managing logs better. I think a lot of the things that in many cases are not new practices but ones that we need to reaffirm the importance of and really double down on making sure those are implemented.

I think many of the guide and practices across this EO are intended to inform improvements in many of these critical areas for federal agencies, and I think that will extend in some ways potentially through procurement practices of the federal government to other organizations as well. From our perspective at NIST, the resources we put out will be applicable to federal agencies, but certainly voluntarily to any other organization as well to the extent that they provide value and address a challenge that you face.

This is really my last substantive slide. In some ways this is a public service announcement. We are really trying to emphasize the importance of preparing for a future migration to post-quantum cryptographic algorithms. I won't go into bits and bytes, I'm not going to throw out numbers, all the crazy math with encryption, because most of that I don't understand.

But the issue here is that look, from time to time there are cryptographic weaknesses or dependencies or just technological evolutions with new technologies that will necessitate us as a broad stakeholder community to replace legacy cryptographic algorithms. Replacement of algorithms based on past experiences with other algorithms over the years can be disruptive to operations, and it can in some cases take decades to complete.

So while we continue on a process to standardize post-quantum cryptographic algorithms, and again these are algorithms that as quantum computers and computing becomes more powerful, at some point those will become powerful enough to break many of the algorithms that are in use today.

So we are in the midst of a competition similar to what we did with the advanced encryption standard years ago, to select and standardize on new algorithms that will be resistant to quantum computing in the future. This is a long-term project, we anticipate the standardization of those happening within the next two years, I'd say 2022-2023 timeframe.

There are things organizations should be doing today to start preparing for that migration, so before we have algorithms, before they're standardized, before they're built into technologies, things like understanding where you're encrypting data today, what are you using to encrypt those, how long do you need to protect that data, we're working on potentially developing a playbook, very specific playbook that can help guide organizations of any shape and size, if you use encryption, to protect your data, developing a playbook to help guide that inventorying process and some of those migration preparation activities. So again, just a little bit of a public service announcement, but we try to take full advantage of any opportunity we can to highlight that.

And again, we're always open and eager to engage, plenty of ways to engage with us. Rather than go through this, certainly the link at the bottom here will take you to a lot more detail on how to best engage with us in a variety of different areas. So with that, I apologize for being a little long winded, I will stop there and look forward to your questions.

Nick Coussoule: Thank you Kevin, I very much appreciate that. I will open it up to members of the committee to ask questions, but I'll take my preference to start first. I have one that's directed to either of you, and it's a little more generalized. I think a historical approach to cybersecurity was a little bit about how do we build the walls higher and thicker and how do we build the moats deeper and wider. It

was all about keeping people out. And by no means has that diminished, but there's also the practical reality of there's all kinds of negative events that happen.

What are you seeing either from a what's happening in the industry or potentially for recommendations or guidance to people to get faster and better at identifying when they've been hacked and mitigating and coordinating that risk or remediating that risk? So a little bit more of a focus on the reality of getting hacked or compromised versus we try and spend all of our dollars in stopping that. So what are you seeing from an industry perspective, or you recommend for people to think about that in a slightly different way.

Suzanne Widup: I think the most important thing is that you're able to detect when something is happening. And we spend all this money on systems to supposedly detect just that, but have they been tested, have you actually been able to identify by actually throwing some kind of attack at these systems what it looks like when they actually are being attacked, because if you can't recognize it then it's not going to be an actionable alert, and you're not going to find it when people are actually attacking you, and I think that's really important.

Kevin Stine: Definitely agree with Suzanne. I think a lot of what I'm seeing or hearing, and we're trying to do this at NIST as well, is a lot of the discussion is starting to move more towards resilience as opposed to just pure prevention or protection.

I think we've all realized over the years, and certainly a lot of the recent high visibility high profile events, bad things do happen, can you continue to operate critical mission functions in the midst of those types of events and issues. So focusing not just on the traditional kind of protection and detection if you will, but really can you be a resilient organization in delivery of your mission and business objectives.

I think one of the things we observed when we were developing the cybersecurity framework, again go back to 2013-2014, is if you're familiar with the taxonomy of the framework, we have these things called the five functions, which in some ways represent big buckets for the universe of cybersecurity very simply stated.

You've got identity, protect, detect, respond and recover. And part of the framework development process was across those and sub outcomes within each of those buckets is let's understand what are the existing standards and practices that can be used.

And probably it's no surprise there are a lot in the protect side, a lot of emphasis on protection, a lot of standards, a lot of guidelines, a lot of practices, a lot of technologies. Quite a few less in the detection side. The response and recovery were almost empty. And that is not just looking at NIST resources, but really broad community resources in the standards and the guidelines space.

That really was, when you see the data if you will on paper, that was really a wakeup opportunity for us to really take a hard look at our portfolio at NIST to say okay, how can we begin to fill some of these gap areas with the resources that can help organizations really be much more resilient in their cybersecurity posture, and really with an eye toward helping them to be resilient in the context of their missions and business objectives.

Nick Coussoule: I would ask the committee members to raise your hand if you have a question. I think I see one. Val?

Valerie Watzlaf: I think this is for Kevin. I love all of your resources. I'm especially excited to see the one on telehealth. I guess my question is can you discuss some of the major issues that you see in relation to telehealth security that you found maybe through that particular insight or the research that you did in that document, or maybe the top two areas or whatever you can provide.

Kevin Stine: I'll certainly provide some of my thoughts, and we have a team of folks that are working hand in hand with many industry counterparts in the sector that I'm sure can be much smarter than I can. When I think about telehealth, certainly there's the technology side of things, you think about different broad category of IOT and the security that goes along with those types of technologies that may be deployed or used in a lot of different settings, including in a patient's home, or in some, what I'll call a nontraditional care setting if you will, not in a doctor's office or hospital. So there's kind of the device security considerations and challenges as well as kind of the security consideration challenges in those operating environments.

The other would be the reality that there are many individuals that are involved in a telehealth environment. To include the patient as a part of that in terms of having these types of technologies available where they may be under their care or control in some ways. And I think that certainly there's certainly benefits and opportunities there, but there's certainly challenges that come along with that.

So from our research and our practical application perspective, how do we help improve the cybersecurity of that really broad architecture or implementation landscape, when you're including within a traditional care setting in potentially a patient home or something along those lines, and then the diversity of the technologies that are used there.

Valerie Watzlaf: Thank you.

Nick Coussoule: Other questions? Let me ask another one. I guess I'll start this with Suzanne. When you do your surveys, and there's lots of good statistics and good information on there, it's always an interesting question for me, what are you either hearing or seeing that doesn't show up in the surveys, or that you think are either thematic that might be coming or what's new out there that doesn't necessarily show up in the bulk or the higher level of the survey? Are you seeing all the signals about what's new or different that's coming down there that you can help enlighten us with?

Suzanne Widup: First of all, these aren't surveys, these are actual cases that are worked by forensic people. But yes, one of the things that I have seen trending upward is you see the ransomware where they take a copy of the data and they're using some kind of public shaming of the victim to try and get them to pay.

Well, I've also started seeing that with hacking, not just with malware. So they haven't encrypted the data, but they have taken the data, and they are threatening to release it. It's the stepsister of the ransomware tactic that they've been using. And I think that's happening more often now too.

Nick Coussoule: I think obviously with the healthcare data and some of the sensitivity to that it makes it very much apparent in our industry as well. Kevin, thoughts on that as well?

Kevin Stine: I'll echo Suzanne's comments, I definitely agree with them.

Nick Coussoule: Any other questions from our committee members or staff? Valerie?

Valerie Watzlaf: I have another one, just to follow up. On your resources, there are so many that are so good. But I don't know that everyone knows about them. So I don't know, how do we help you I guess or help to disseminate them better or get them out so that people really are using them, or do you feel that it is good enough, that you're able to communicate them and get them out as well?

Kevin Stine: I definitely don't feel that it's good enough right now. I think over the years our mindset at NIST has had to evolve from we can put the resources out and let those speak for themselves, to we need to be much more proactive in getting the message out there.

A few thoughts on that. One is we are a relatively small federal agency by federal agency standards. So when we think about our workforce we have our own cybersecurity experts and expertise, but we really think about our workforce being hundreds of thousands or millions of individuals because of the process we use to invite folks from all around the world and all sectors and all sizes of organizations and governments and nations to contribute to our efforts.

And I think through those far-reaching tentacles, that's a great way to start. And that's the approach we try to take with everything we produce, every resource that we produce, whether it's a standard or guideline or practical application. Talking with groups like this is another great opportunity.

I think part of what we also need to do though, and I think we're starting to do this, and we probably need to be much more aggressive, is not just put out documents, so not just put out the volumes that are this thick that have a lot of great detail in them that's very important, but that's going to, those will not be useful or as helpful as possible to all audiences.

So we're really trying to take a much more diverse view of the resources we put out, so not just the voluminous special publications, but videos, and infographics, and cheat sheets, and quick start guides, and those types of things. So then in some ways we can help to meet people where they are, meet organizations where they are, and if nothing else they can provide a teaser where they can always go back to the foundational resources that we have with all the great details to give them more information.

This is an area where I'm always eager to get feedback on what we can do better, what's working great, where are some areas where NIST if you really did it this way this would reach a whole new community, so I'm always eager to receive that type of feedback.

Valerie Watzlaf: I think you mentioned too that you are doing more of a playbook for the encryption around the algorithm part. So I think that's another example. Thank you so much.

Nick Coussoule: I guess as we presented this morning, earlier this afternoon, was talking about the transition from a focus on data security to data availability to data integrity, you're now focused on a transition into the historical kind of attack models of doing that, what are you seeing now that are either new threats or potentially things that can be done to counter some of those threats in regards to things like the example earlier about inserting into actual pictures, to do some of the spoofing models. Are you seeing any of that either in the analysis of the events and activities, and I didn't mean survey, thank you for correcting me there Suzanne, or even in some of the research that's being done at NIST?

Suzanne Widup: I have not seen that kind of attack as yet, and part of it may be if it is happening it's just not either making the public notification that we can see, or it's not something that our partner is seeing. It doesn't mean it's not happening, it just means we don't have visibility into it.

Kevin Stine: I would agree with that. From our perspective ransomware is a great example while it's occurring here nothing, you're seeing kind of the trends towards ransomware as a service, so there's really a market for these types of malicious capabilities. So they're very entrepreneurial as well. I don't know that that's a brand-new thing, but we're certainly seeing that play out for sure in interesting ways. There will always be a next, new challenge or threat vector for example.

From my perspective, and this is the importance of that life cycle spectrum of that early stage research, how can we begin to look at the research opportunities now to analyze or try to predict the direction technologies or the threat environment may go so we can begin to have the guidelines and the standards and the technologies really in place so by the time they're a little bit more prevalent on the negative side that we have the resources to help organizations.

Nick Coussoule: At the risk of channeling Denise's questions earlier, if you are to make a recommendation or suggestion for what NCVHS should consider for recommendations to the secretary, are there one or two things that stand out in either of your minds about what we could focus on or try to encourage?

Suzanne Widup: I think that one of them is that security is not a one size fits all proposition, it needs to be risk based so that people can tailor it to their own environment. That said, I also think that detection and response need to be prioritized, because they are really your most important things.

You need to know if you are being attacked quickly, you need to be able to respond appropriately. Incident response plans are very important. One of the things that we do with our research is show you the most likely ways you're going to be attacked, and so if you don't have an incident response plan to handle those kinds of things, that's a great place to start.

And then finally with ransomware the importance of being able to separate your backups from your regular systems so that if an attacker gets into your system, they don't also compromise your backups because they're actively looking for that, before they trigger the encryption they will see if they can get to your backups as well, and if they can then they're going to make sure they encrypt those as well. So it's very important to keep those separate.

Kevin Stine: We frequently think about cybersecurity in the context of cybersecurity is not a problem to be solved, it's a problem to be managed, at least that's kind of our current thinking today. So I definitely

agree with Suzanne's point, this ultimately is a risk management issue for every organization, every federal agency, every agency at any level. And every organization large, small, and everything in between.

So I would emphasize the need and the importance of risk management approach. I would emphasize the importance of a resilience mindset with an emphasis on response and recovery, but at the same time emphasizing look, there are basic practices that we've all known about for many years, like access control. Least privileges.

Some of the foundational principles in cybersecurity that if implemented properly would go a long way in helping organizations to be in a better position to not have things that are happening today happen to them. So getting back to the basics and stressing those. Frequently people talk about cyber hygiene, not my favorite phrase but that's okay. The other two things I would mention real quick, there's always a workforce dimension, not just in the cybersecurity workforce but I think increasingly in the privacy workforce, in the context of this discussion.

And then finally is a little bit more forward leaning is understanding the impact that new technologies are going to play with respect to cybersecurity and privacy. And I'm thinking of things like artificial intelligence and machine learning. Increasingly we're looking at AI and machine learning for example in the context of how it can be used to help security, and how do we secure those. So kind of looking at it from both sides of the coin.

This is very much a research area for us right now, and certainly others are looking at it as well, but I think we want to not lose sight of some of these new technologies and technological evolutions that are going to have an impact on the way we deliver care in the healthcare setting.

Nick Coussoule: Excellent, thank you both. Any other follow-up questions from our committee members or staff? Okay. Well, I will thank both of our panel members for the presentations and the questions, very informative and thought provoking, in some ways scary, but again that's what we're here for, thank you again very much. I'll turn it over to Melissa.

Rebecca Hines: I just wanted to say Melissa and Jacki, that I know Vickie has to leave early today, and she does have some thoughts for the discussion later. I don't know Vicki if you want to share your thoughts to contribute to the subcommittee discussion later, or whether you'd prefer to do that by email.

Vickie Mays: I don't want to be disruptive now, since I can't be here at the end, if we just share the stuff that I put in the chat so that they can have it, so the discussion can be kind of all things at the same time.

Rebecca Hines: Sure. Vickie has some nice very specific thoughts, so I will send them by email to the subcommittee so that you can include them in your discussion when we get to the subcommittee discussion towards the end of the agenda. We are a little ahead of schedule. Melissa, Jacki, Nick, any thoughts? Would you like to take a break until 3:15 when our next panel is scheduled to begin?

Jacki Monson: I think that's a good idea. I don't know about you all, but I feel a little fatigued sitting in Zoom for such a long time, so I think it would be good to have a little bit of a break.

Rebecca Hines: That works out great then. We'll take a pause until 3:15 when our next panel is scheduled to start. Enjoy your pause.

(Break)

Panel IV – Federal Perspectives on Security Infrastructure and Enterprise-wide Risk Management in Healthcare

Melissa Goldstein: Hi there. We are excited to have this afternoon's panel, our final panel of the day. I see that Julie has joined us and Tim. I see that you are here as well. I will quickly introduce you both and feel free to add to it, add to my introduction.

This panel is on federal perspectives on security infrastructure and enterprise-wide risk management. As I mentioned, Julie Chua will join us. She is with the Office of Information Security in HHS. She is the director of Governance, Risk Management, and Compliance Division within HHS and within the Office of Information Security. She is also the federal lead for the implementation of the Cybersecurity Act, CISA of 2015, which we have also – which we talked about in other panels today for Section 405D, aligning health care cybersecurity approaches.

We also have Tim Noonan, who is the deputy director of the Health Information Privacy Division at the HHS Office of Civil Rights, also mentioned several times today. Tim is the director of the division that administers and enforces HIPAA, the HIPAA Privacy, Security, and Breach Notification Rules, as well as the Patient Safety and Quality Improvement Act and Rule, using investigations, rulemaking, guidance, and outreach. Tim has been at OCR for a while in several different capacities. We are very excited to have both of you here today.

Julie, if you are ready, we can go ahead and start.

Julie Chua: Thank you so much, Melissa, and thank you for inviting me today to talk about what we re doing with our health care and public health sector partners and also some of the initiatives that are trying to address cybersecurity within the HPH.

The first few slides that you will see – the next two slides are really setting the stage of what we are seeing in terms of the current state of cybersecurity in the health sector and specifically what you are seeing right now on the slide is of course ransomware is a big challenge. It is a threat that we are facing within the sector and some of the astounding numbers is that the attempt in 2020 has risen to 123 percent. That was in a cyberthreat report. The other thing is of course the associated costs to ransomware attacks. It has doubled in number from 2019 to 2020. As you can see here, it is about $20.8 billion in downtime. The reason why they call it downtime is there is tail end types of costs for ransomware or any cyber incident. When you get into the response and recovery stages, it is taking a long time to get into your desired state or your state before a cyber incident has occurred.

I think before I move on to this one here, the key takeaway also from one of the slides is that the access to files and data within health care settings is also a challenge, meaning it is either instant access and it is not rule-based access where it is a need to know and the reason behind that is, as we all know, we, in the health care industry, need information for quality of care, continuity of care, health outcomes, and

the delivery of that care. There is a bit of a challenge in terms of really putting forth and implementing certain cybersecurity best practices within health care settings. That is one of the things that is making it challenging to implement and really permeate throughout health care organization.

Another thing also with this slide that you see here is cyber safety is really for us patient safety. It is an issue that is not just within an IT department. It is not an IT issue that only an IT department would and should be addressing. And we should also be looking at this from an enterprise-wide lens. We will get into what enterprise means and why enterprise risk management is an effective organization-wide approach.

What is ERM and why is it very important in terms of addressing cybersecurity risks within health care settings and actually for all types of organizations? ERM is looking at all significant risks. It is a combined portfolio of interrelated risks that an organization is tracking. It also advocates a guiding principle and risks are interrelated. It is tied to mission impact, and it also normalizes the risks across many domains.

When we say interrelated portfolio, that is your privacy risks, cybersecurity risks, reputation, operational. If you are a grant management or a grant funding organization, your grant managements, financial, IT, all those risks that an organization looks at. What we are trying to say is cybersecurity should be embedded into that portfolio.

Again, this cannot be stressed enough where cybersecurity risks are becoming or is already a patient safety issue. To address this, we must begin thinking of cyber risks as enterprise-wide risks.

As you can see here as it is populating, it goes through all the different kinds of risks that an organization looks at and tracks as their enterprise-level risk.

The next slide is really looking at how ERM impacts the health sector. As I think and I think I am sure also with the statement, most of the audience today knows that HHS is the sector risk management agency for our sector. And that means we are responsible for raising awareness about risks, inclusive of cyber, and it is also means that we have a responsibility to manage those risks and provide assistance, awareness, the resources to our private sector partners about how to manage those risks including the cyber risks that we face.

One thing that we are doing is as an agency, we are advocating of course for cyber ERM integration. There are several actions and activities that we have on the federal side of things. That is why on this slide you are seeing that on the left side, we are showing that cyber and ERM integration – we are working on those activities within HHS. By association and by extension, those things that we are doing internally within HHS, we are able to advise, share best practices, and continue to advocate that integrating cyber and ERM is a good best practice.

On the right side, you will see all the subsectors for the health sector and that essentially by strengthening the cyber and ERM integration, it will help ultimately improve the patient health data, security, and privacy and reduce the risk of these disruptive cyber events.

Another thing that is good to mention on the federal side, which is also helping our engagement and our assistance with the private sector partners is there is an interagency community of interest that HHS co-

chairs with NIST. It is comprised of over 100 federal agency representatives now. And one of the deliverables of that interagency effort is the new special chapter on cyber ERM integration that is located within the federal ERM playbook. I choose to highlight this with this council or meeting because it is informing the activities that we have with our health care and public health partners especially with the cybersecurity act of 2015 implementation and activities under that.

The last thing I am going to say about federal activities and advocating and pushing awareness for cyber and ERM integration is NIST also published recently in October of 2020 a NIST interagency report, 8286, specifically on integrating cybersecurity risk management with enterprise risk management. That is another step forward and a milestone towards raising the awareness of this very important practice.

The next few slides are now going into how are we helping right now and how are we addressing increasing awareness and providing resources to the sector. The Cybersecurity Act of 2015. There is a Section 405 that is specific to health care cybersecurity and strengthening the posture of our sector. And what we are doing right now is we have a task group that HHS convened in 2017 and it is really tasked to address the mandate for this, which is to develop a common set of voluntary, consensus-based, industry-led best practices. It includes guidelines, methodologies, procedures, and they are all voluntary to ensure that our health care organizations have the resources and have the information they need to address the cybersecurity risks that we face.

The makeup of this task group. We have been very lucky with the participation from across federal governments, state, local, as well as our private sector partners and we have a good representation across CIOs and CISOs as well as medical professionals, health care providers, nurse practitioners, hospital administrators. We have had privacy experts as well join the task group to inform the work that we do there.

The cornerstone publication that we released in 2018 is called Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. It is called HICP for short, quite appropriate for our sector. However, the strength of this publication is the makeup of the task group. It was written and developed with the lens of health care first and then cyber so that all health care organizations no matter if they are small, medium, and large can find themselves in this publication and it is also stratified with technical volumes that are meant for small and then for medium and large. This is being updated right now within the task group and it will go through the same rigor and review and clearance process as did the first version.

Within this slide, you will see some of the additional products that supports enterprise risk management and how we are making it more concrete for our stakeholders. The left column shows your HICP publication. As I mentioned, there are technical volumes in there. We already advocated for treating cyber risk as enterprise risks within that publication in 2018. We are continuing that thought process and that advocacy into one of our newer publications that are still under development where it really focuses on enterprise risk management and cyber risks.

All the other education and awareness products we have come in the form of webinars, posters, and also quick facts through – and those are distributed I should say through our social media platform such as Twitter, LinkedIn, and Facebook.

I believe that is my last slide. Yes. Again, I am very fortunate to have some time with the committee today. I hope this was useful information. I am not sure if there are any question-and-answer time for that. But I will turn it over back to Melissa.

Melissa Goldstein: Thanks very much, Julie. We will be taking questions from the committee members after Tim speaks as well. Thank you.

Tim.

Tim Noonan: Good afternoon. I am Timothy Noonan. I am the deputy director for Health Information Privacy at the Office for Civil Rights, Department of Health and Human Services. Thank you for the invitation to speak today.

OCR's role in administering and enforcing the HIPAA rules gives us an informed perspective on the state of the health care industry's compliance with the HIPAA rules and the overall protection and security of the health information that is entrusted to their care.

Today, I thought I would discuss some of the trends that we are seeing in our large breaches of unsecured protected health information and the findings from our last round of HIPAA audits on risk analysis and risk management, some common themes in OCR enforcement actions in breaches caused by hacking, and then identifying some of the resources that OCR has available to support cybersecurity. I can do all of this in about 15 minutes or less so that we will have plenty of time for questions.

OCR has seen a substantial increase in the large breach reports received over the last five years. A larger breach report is breached affecting 500 or more individuals. We used to say we would average one large breach report a day. But as you can see, there has been a substantial increase from 2016 to 2020. We see a 98 percent increase from 2016 to 2020. And then just from 2019 to 2020, a 27 percent increase.

What types of breaches does OCR receive and how has that changed over the years? The pie chart on the left shows the cumulative data since 2009. You see hacking is the largest area, 36 percent. Physical theft and unauthorized access or disclosure are also significant, roughly 27 percent each. The chart on the right shows 2021 data current through the end of June. You see here that hacking is by far the most common type of breach report to OCR. It is 72 percent. And you can see the movement form physical theft to hacking as the type of breach that is being experienced in health care entities.

Maya Bernstein: It is Maya. Sorry to interrupt. Can you just explain 2009? Is that just because that is when the rule went into effect and that is when you started collecting data? What is the significance of that date in particular?

Tim Noonan: That is when OCR took over enforcement of the HIPAA Security Rule.

Maya Bernstein: They switched over from CMS.

Tim Noonan: Yes. That is the start of our data. The data shows that hacking is the most likely type of large breach that a covered entity will experience. This is consistent. In 2020, hacking was 68 percent of the type of breaches that were received by OCR.

Here we see similar data for location. The pie chart on the left shows cumulative data again from 2009 to the present or last year I should say. Email, network servers, paper records. They are the largest categories of breaches by location. For 2021, you see that network servers and email are the dominant locations. For email, it is the phishing or impermissible disclosures as the most common location for HIPAA breach involving email and then network servers are increasingly becoming the location of large breaches reported to OCR.

Overall, this data highlights the increase in reported breaches to OCR. The rise in hacking as the cause. And then the rise in emails and network servers as the primary locations. That is where all the action is in cybersecurity and OCR enforcement.

Here, another way of looking at the breach reports involving hacking. Here, you can see the rise in breach reports to OCR involving hacking and particular ransomware. As the number of reported breaches to OCR has gone up so have the number of hacking incidents as the cause of breaching. As I said, hacking is the largest sources of breaches of unsecured PHI that are reported to OCR.

There has been a 267 percent increase in large breaches reported to OCR involving hacking from 2016 to 2020. For ransomware, it is even more significant, 452 percent increase during that same timeframe. This is the largest cybersecurity threat facing the health care industry today.

Another way of looking at the rise in email is the location of breaches. Here, you can see from 2016 to 2020, 381 percent increase. Very popular attack vector. We will be talking a little bit more about that in the scope of some of our investigations.

Although not as dramatic as increase in email as a location in network servers, there has been 184 percent increase since 2016 as the location for large breaches.

In addition to our data regarding our large breaches that are reported to OCR and the subject of our investigations, I also wanted to talk a little bit about our last round of HIPAA audits and some of the data that was collected. Here, you see some of the data from the 2016-2018 audits that we performed. We conducted audits of 166 covered entities and 41 business associates.

The audits – they give OCR a perspective of the industry that otherwise does not come to our attention through the filing of complaints of the reporting of breaches. And we examined the oddities compliance with the HIPAA rules in several areas. But for today, we will focus on risk analysis and the risk management requirements in the HIPAA security rule.

Each auditee received a rating for each HIPAA standard or implementation specification that was examined. And the ratings ran from one to five. One is that the entity is in compliance. That is your A. Two is entity of substantially in compliance. We will call that a B, maybe C. Three, the entity made attempts to comply, but these attempts were inadequate and it gets progressively worse. Four was negligible efforts to comply and five is entity did not provide evidence of serious efforts to comply with the requirements.

For our purposes, we will consider the ratings of one and two to be general compliance. You can see regulated entities. For risk analysis, regulated entities are required to conduct an accurate and thorough

assessment of potential risks and vulnerability to the confidentiality, integrity, and availability of electronic protected health information that they are holding. For risk analysis, you can see that the categories one and two. For covered entities, the percentage that were in compliance was 14 percent. For business associates, it was slightly higher at 17 percent. The remaining percentage of audited entities' efforts to comply with the risk analysis requirement in the HIPAA security rule were inadequate or worse.

For risk management, the HIPAA security rule says regulated entities are required to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. After you have conducted a risk analysis, you have identified the risks and vulnerabilities. You are to implement a risk management plan to bring them down to a reasonable level.

Here, we see the results from the HIPAA audits were similar. For covered entities, again, adding the percentages for ratings one and two, it was six percent, six percent compliance. And for business associates, it was 12 percent.

We published last year by the way in industry report. That is where this data is taken from. It goes into much greater detail. It is a benefit to anyone. Rachel Seeger or myself. Just let us know and we can give you a copy of that report. It is also available on our website.

The audits confirmed what we have found in our enforcement program. Our enforcement program investigates complaints, compliance views and breach reports reported by covered entities. Within our enforcement program, the failure to conduct risk analysis and risk management are the most common violations that we identify. Unfortunately, the audits reveal that what we are seeing in our enforcement investigations is consistent throughout the regulated industry. The basic building blocks of cybersecurity, risk analysis and risk management. They are not present in the regulated industries. They are making themselves attractive targets for ransomware hackers and other threat actors.

Here is a list of the completed enforcement actions involving the HIPAA Security Rule for the last two years. This is not everything that OCR has completed in terms of investigations. It leaves out our right of access initiative, which is completely separate. But these are key cases where we obtained a settlement with regulated entity, and it involved the security rule.

For today, I would like to highlight some of the cases that have a common theme. The Premera Blue Cross, CHPSC, Athens Orthopedic, and Excellus Health Plan cases. All of these cases were caused by hacking. That is how the cases came to OCR's attention.

As I noted earlier, hacking is the greatest cybersecurity threat to the health care industry. OCR has made that an enforcement priority over the last few years. These cases with the entities identified, there is a general fact pattern that runs throughout. A hack occurs. Sometimes it is through a phishing email and the installation of malware. Sometimes remotely through the compromise of user's credentials. Exfiltration of data occurs. The hack and the hackers continued access to the information system is undetected for months. And the net result is that the individual's protected health information is disclosed to a cybersecurity, or it is posted on the Internet.

Some general common themes in OCR's investigation of hacking cases that I think highlight the lack of

sufficient risk management and the general cybersecurity risks to regulated entities. First, in the cases of identified, there was a lack of an enterprise-wide risk analysis. This continues to be one of the most common HIPAA security rule violations. It is the building block of all the other HIPAA security rule requirements. Entities have to know all of the places where their electronic protected health information is held so they can probably assess potential risks and vulnerabilities to it. If you do not know where your EPHI is held, you cannot protect it. It is that simple.

Second, entities need to respond quickly when there has been an intrusion into their IT system. This requires implementing procedures to regularly review system activity such as audit logs, access reports, and security incident reports. Hackers cannot be allowed to just nest in an entity's IT system for months undetected, installing malware, and exfiltrating EPHI.

Melissa Goldstein: Tim, this is Melissa. Should we be on the next slide now? Just checking.

Tim Noonan: No. General themes. Thanks.

Third, access controls. Entities should implement multi-factor authentication especially for remote access as this continues to be a very popular and large risk attack vector. Unique user IDs and ensure that access to EPHI is limited only to those persons or software programs that have been granted access rights. We tell the regulated entities, do not make it easy for hackers to have unfettered access within your system.

Fourth, audit controls. Entities are required to implement hardware, software, and procedural mechanisms to record and examine information system activities. Entities need to know who is accessing the EPHI they hold and when. In a lot of instances, entities cannot even tell when the hack occurred because they do not have audit capability in the information system that was hacked. They do not even know when it began. They have to take a guess. That is not good.

Here are some best practices that we recommend for cybersecurity, and they track with the HIPAA Security Rule our requirements and the common themes I just discussed. The only other item I would emphasize here for today's purposes that I did not previously mention is workforce training particularly when it comes to identifying phishing emails and knowing the procedures for reporting a suspect security incident.

Phishing emails is becoming very common. You saw the rise in emails as an attack vector. You can have all the greatest security in the world. If a workforce member is clicking on an email, sending them a Christmas card in July, there is going to be problems. Having a dedicated training mechanism in place. Perhaps running sample phishing tests within a regulated entity's organization can really improve the workforce members' understanding and awareness of phishing emails.

As we have identified risk analysis and risk management as being key deficits within the health care industry, we have tried to provide tools to help regulate entities be better prepared in responding and fulfilling basic HIPAA Security Rule compliance.

First is the Security Risk Assessment Tool. This is a self-contained operating system independent application that is available for download. It can be run on various environments, including Windows

and Apple. It takes you through each of the HIPAA requirements by presenting a question about the organization's activities with a yes/no answer. There are about 156 questions. It is a great way of identifying all the locations where EPHI is stored and being able to start assessing the risks and vulnerabilities to that EPHI and an order of priority so that you are able to transition then this identification of your vulnerabilities into a risk management plan. That is available on the HHS website. It is a great tool for entities to support their creation of risk analysis and risk management.

We also publish a cybersecurity newsletter. These newsletters address threats within the industry as well as identifying helpful best practices and explanation of security rule standards. Our summer 2020 newsletter addressed HIPAA and IT asset inventories as a useful tool to assist in developing a risk analysis. And in fact, we issued a newsletter today, this morning, discussing information access management and access controls.

Other recent topics include preventing, mitigating, and responding to ransomware, advanced persistent threats and zero-day vulnerabilities, managing malicious insider threats, phishing, et cetera.

Finally, we also have Security Rule Guidance materials. This includes guidance on implementing security rule risk analysis requirement, information about security for mobile devices, understanding and defending mitigating the threat of ransomware, NIST special publications on information technology security, Federal Trade Commission guidance and security risks from peer-to-peer file sharing applications and FAQs on minimizing the risk of medical identity theft.

The trend we have observed over years is there has been significant movement from paper-based breaches, the records that end up in a dumpster or physical theft break-ins, a result of medical records being stolen. It is all cybersecurity, and it is all hacking in ransomware. The risk that you saw in the breaches report to OCR is primarily triggered by hacking. That is where it has been growing exponentially and that is where we have been focusing our resources both through the HIPAA audit, our current investigations, and then developing more guidance-related materials, including this morning's cybersecurity newsletter.

With that, I am happy to open it up to questions for Julia or myself.

Melissa Goldstein: Thanks very much, Tim. We will open up now for questions from the subcommittee members and the committee members for those of you have joined us. Please raise your hands. In the meantime, as we have the hands going up, I would like to ask both of you a question that Jack has started us off with this morning of what we could do as a Federal Advisory Committee and making recommendations to the secretary in basically pursuing the objects and the mission of both of your elements of HHS. How could we help? What recommendations could we make? What areas could we study in more detail? How can we help you?

Tim Noonan: I am happy to answer first and get some thoughts on the table. Our current statutory authorities I think are sufficient with respect to our enforcement authority. It is a little bit of a challenge for OCR to get at the answer as to why. Why are we not seeing greater compliance within the regulated industry? There is an affirmative duty for regulated entities to be in compliance. It is not a matter of you need to come into compliance when OCR catches you. It is you needed to come in compliance. In the

case of the HIPAA Security Rule, that was published in 2003. We are well past 15 years of it being in place. This did not happen yesterday, last night, et cetera. It has been in place.

I think part of it is the challenges. It is a huge industry. There are entities of big and small that do not believe there is a great likelihood of them being caught. We have tried to make a little greater focus on smaller entities particularly with our right of access initiative. We are not just fishing in the deep waters. We are not just pursuing the largest, the biggest entities. It is trying to get the message out that the compliance expectations, the requirements extend to the entire industry, and we are not just fishing in the deep waters looking for big entities. It is everybody.

The dental industry, for instance. We have had a lot of challenges with dentists that do not appear to take their HIPAA obligations seriously.

I can share with you some of the things that we are strategizing, trying to implement as part of our overall plan. We are continuing to increase our enforcement activity. We have increased our staffing to support more of that. There will be additional HIPAA audits that allow us to take a look at other segments of the industry outside of what we are seeing in our enforcement program and also be a little more perhaps proactive in that we are looking at an entity before there is a reported incident, giving rise to a breach or before someone has filed a complaint.

And then we are engaging in significant outreach efforts. We do massive amounts of outreach. In fact, it is one area where perhaps it has improved as a result of what has occurred with COVID-19 and the greater use of webinars. It has allowed us to be able to participate in more events because you do not have the physical travel limitations. You cannot be in two places in one day. Nowadays, you can. We are trying to take a comprehensive view. It is not just the stick coming after folks and more HIPAA enforcement. Although I do think that is part of the solution. It is also increasing the education of it.

One area is – the HITECH Act. As you recall, that was passed in 2009. This is just me speaking. This is not anything that is an official statement from OCR. Just my own perspective. I spent 2009 and I think we have seen instances where the penalty tiers and the caps and the range of civil money penalties. Perhaps that has not kept up with the state of the industry as it has become this multi-billion-dollar industry. The caps – it is 1.5 million for a violation. It is adjusted for inflation. It is a little bit more than that. But that is for willful neglect uncorrected. And perhaps it is time to revisit some of that. It has been more than ten years since those caps were created. And that was in response I think largely to the sense that the original penalty mechanisms in place for HIPAA enforcement were insufficient for the regulated industry. That could be an area to explore. I would be happy to have further conversations or have a more official OCR position.

Just in terms of the landscape and additional legislation, I am not sure that additional legislation always brings clarity or makes things – is going to change things dramatically. The laws are already present. They are already in place. It is just a matter of education and enforcement, I think, to compel greater compliance. It is something we are very interested in too. It is discouraging to see the results in the audit and the results in the HIPAA enforcement program. There are just folks that remain largely ignorant of their HIPAA responsibilities. That is to the detriment of patients and individuals everywhere.

Julie Chua: There are a couple of things that, Tim, you mentioned that I would like to tease out a little more. The one thing about risk management and risk analysis is I think for our sector, it is oftentimes seen as very vague and very cumbersome to do. I think that lends itself to not knowing what they are supposed to be looking at and at the same time we have heard that from the HIPAA Security Rule perspective that is why it is not prescriptive so that it is knowing your own risk environment and how you would be looking at your threats, the exposures to those threats, and then how you want to prioritize and mitigate the risks now that you know that you are vulnerable to certain things.

I think it is education, I would agree with that, and making sure that it is not just the IT and the information security professionals that are getting that education, but also those other roles within a health care setting inclusive of your board of directors, inclusive of your emergency management domains or teams within a health care setting because when we engage with our stakeholders through 405(d) efforts mainly is that is what we hear. There is a certain subset of maybe more larger, integrated health systems where their CIOs, their CISOs, that community is collaborating, for example, with their emergency management community. All the more now because they are seeing that cybersecurity is and should be looked at in the lens of all hazards, meaning there are certain things that can be gleaned from existing emergency management frameworks that can be applied to cyber.

One thing that I have also heard is it seems like the cyber aspect of it gets folks to just pause and freeze. Where there are certain things that are best practices across the board that can be included in a response or in the risk management lens that goes through the NIST framework of identify, protect, and detect, respond, and cover. That is a universal framework and that is one thing that we also encourage our stakeholders to do.

But in terms of the specific question about what can this committee do? I think it is more of amplifying, amplifying what OCR is stating in terms of these are the things why risk management and risk analysis is important and everything else follows because you have that foundation or amplifying the work that 405(d) program is doing because, one, we are mandated to do this. It called for HHS to convene this public-private partnership and we tried to amplify as we can the best that we can through the Sector Coordinating Council, the GCC. Both councils are kind of saying that there are resources available to you to actually try to find yourself in this mix of cyber incidence, cyber notifications, and as a health care entity and as a sector, I would say small, medium organizations are those that most need this help. Similar to Tim, we are focusing our efforts on reaching those small and medium.

The one thing that we are also seeing is the associations, professional or trade. They help as the force multipliers. They reach out to their members, saying did you hear about this yet. These are things that are available to you. For the 405(d) perspectives and the scope of ours, it is voluntary. That is where it also gets a little tough to advocate and get implementation. But at the same time, I think it is lending itself to being more accessible. In a way, we have heard that from our stakeholders who are trying to implement, adopt fully or in part what we have provided in terms of the HICP document itself.

I think the last thing I am going to say about certain legislation and policy is there is that new bill that passed, amending HITECH so P.L. 116-321. We are still working with our OCR colleagues with that. We are paying attention to that. From a 405(d) lens, we are encouraged by that bill because it calls out as recognized security practices although that is still – we are still trying to figure that out. That anything

that is promulgated under 405(d) is under the definition of recognized security practices.

To me, there is still a long way to go. But I think with that specific amendment, HHS has a huge opportunity to figure things out and get some traction in terms of highlighting and emphasizing the need for more focus on cybersecurity and the risk management piece of it.

Melissa Goldstein: Thank you. Those responses were very helpful. Are there any members of the committee who would like to pose questions now? If not, I will just keep going. I am full of questions.

Our next question is about third parties and the recent – we have seen all of these recent attacks, including over the July 4 weekend on vendors that then affect so many people, so many organizations. I am wondering if the focus perhaps on business associates from the audits that were talking about, Tim, or the focus with the 405(d) groups. Do you see any focus shifting in where I guess enforcement efforts or other discussions might be to third parties and the role of third parties or the vulnerability of third parties?

Tim Noonan: When it comes to HIPAA business associates that we have jurisdiction over them if they are creating, receiving, maintaining, transmitting protected health information to assist a cart entity, they are required to report a security incident, a breach to the cart entity and then the cart entity reports the breach to HHS and OCR.

As a practice, when we get notification of those types of breaches that have occurred at the business associate's facility or they are the primary actor, we open up a compliance review against the business associate. It is the business associate, the primary actor, and the cart entity if following their obligation to report the breach to us, but their connection is really limited to signing a business associate agreement with the business associate and it happened at their place. We look at them both. But we do include the business associate so that they are not getting a free ride and we are just focused on the cart entity and the contractual liability they may have created for themselves by selecting this particular vendor.

The ransomware. It is a scourge that is not limited to the health care industry. We are seeing that everywhere. And business associates that have multiple contracts with cart entities, huge information vendors. They are becoming attractive targets. The Blackbaud breach that we saw earlier in the year. That affected hundreds of entities. It is an area of concern for OCR because it becomes – when you look at the magnitude. The largest breach that we have investigated thus far was the Anthem breach that affected close to 79 million people. That record may not stand for long as these business associates that have the cumulations of huge data through different arrangements with the health care systems become primary targets. We have made hacking and ransomware an enforcement priority and that is where a lot of our investigative efforts are involved. We are also interested in educating. It continues to be education enforcement.

We are trying to be responsive to the trends we are seeing in data and what is happening in the real world. As we see that, we shift our focus. That is how we end up with right of access and hacking as our main enforcement priorities this year.

Julie Chua: A couple of things I would add to that is for the 405(d) Task Group and the effort that we

have been engaged with. Third party was already addressed in terms of the discussion should it make it to the HICP publication. We touched on it quite a bit. I think for this update, we are seeing that we will probably include more of the third=party risk and supply chain also specifically.

And the one thing with the recent managed service provider attack is we saw that coming in terms of making sure that the health care organizations knew the different ways that attackers or attack vectors look like. To Tim's point, the dental community, or the dentist community – they are a huge user of MSPs. We were encouraged at one point when the task group actually had a representative from a dental association. But unfortunately, it fizzled out where he —they did not start coming and getting into the conversation and realizing and knowing we do have a stake in this. As most of them are usually small clinics and I would say for health care providers, you have one or two clinic doctor offices where they are everybody. There is IT. There is the building. They are everyone. I think that is resonating more when we say you have a role. You have to know at least basic things.

One of my slides actually included that two-thirds, I think, of organizations do not change passwords. It is very simple. It is mind bobbling, but I think people just toss that aside because it is just a password. I cannot possibly change it every two weeks or whatever it is that your risk posture appetite is. Yes, that is a huge challenge for health care settings.

As we know, we are consumers of a lot of different types of technologies, emerging technologies. And from the federal side of things also, the new executive order that came out, 14028. It has a huge section on software supply chain, and we expect that that will be tracked and monitored by our private sectors partners. We are encouraging them to actually see what they can glean and try to implement also as applicable to them.

Tim Noonan: One other thought occurred to me. I think the largest deficits that we see beyond failing to plan, failing to have risk analysis, risk management in place, it is the multi-factor authentication that would stop a lot of these remote hacks. You need a card and something that is knowledge based and there is not a card. And that encryption. The availability of encryption devices. It is native on just about every operating system, cell phones, apps, et cetera. It still is not being widely implemented. There are mechanisms already in place. They just have to be used. A lot of times it is just a matter of having somebody in the IT department set up the device properly. There is still in their default settings. Audit logs have not been turned on. Encryption has not been enabled. You make yourself a target.

The good news is I think the technology – it is the mouse and the mouse trap. I think the technology is there and is generally keeping up with the threats, but it is not being implemented. That again goes back to assessing the risks and then planning to minimize them.

Melissa Goldstein: Thanks.

Val.

Valerie Watzlaf: Thank you. I had so many questions, but you have been answering them so well. I did want to know a little bit more. I think this was with Tim's data on the risk management and risk analysis part. Are they given or are they shared a score, showing how poorly they are doing or the ones that re doing well? Does that go back to them at all or is that shared with them so that they can see? And then

again, do you have a breakdown? I know that you keep talking about that is more smaller facilities. I think you said you looked at 166 – is it covered entities and I am not sure how business associates. Do you have a breakdown of how that falls out?

Tim Noonan: Yes. There are 166 covered entities, 41 business associates. Our industry report goes into much greater detail. I am sorry. I just do not remember some of the specifics directly.

To answer some of your earlier questions. In the HIPAA audit program, the auditees, as we shall call them, they did receive a specific score as well as technical assistance from OCR. They are aware of our assessment of their compliance. The audits have always been – it is free technical assistance is I think how we have tried to portray it. There is not the risk of HIPAA enforcement. People might be somewhat circumspect. Open up their books and let us take a look if they are fearful that there is going to be a civil money penalty attached because there has not been an underlying breach or investigation to trigger. We want the audits to be voluntary and we want them to share with us so we can share hopefully our good thoughts on the state of their HIPAA compliance. Each auditee received an individual letter that was tailored to our findings as well as the score. They are aware of their deficiencies and what they need to do.

And I will just say for HIPAA investigations, we receive about 28,000 HIPAA complaints a year. We receive over 600 large breach reports. There is a tremendous volume of cases that we have to choose from in terms of when – into what are we going to spend our enforcement resources on as a particular enforcement action. The large majority of our cases are resolved with technical assistance where we speak directly to the cart entity and tell some of the stuff that you have provided is deficient and these are the things that you need to improve or we send a letter, outlining exactly what those deficiencies are. You will see that in some of our enforcement program activity where, in particular, if we have told you in the past what the problem is, what you need to do to fix it, what the requirements of the rule are and then we come back around again through a new triggering event and you still have not implemented some of those things that we told you about years ago, now, we are looking at something a little different. Now, we have an enforcement interest.

Our enforcement interests are eliminating the problem and ensuring or the best extent possible that whatever gave rise to the breach or complaint that happened previously is not still present in the future. It might be a higher culpability tier. When we have given you specific information about your deficits and you failed to take action, that could be willful neglect. That would be a higher penalty tier or it could be a more robust investigation that we are going to do a deeper dive now because you did not implement some of the basic things we told you before and so now we have concerns about the overall state of your entire program. There are some mechanisms that do allow us to follow up.

But I think in general to answer your question, entities that are under investigation and entities that are subject of an audit are informed of what they need to do to come into HIPAA compliance. It really is dependent upon them to take appropriate action. We always direct them to our resources. We have an abundance of resources that are pretty easy to find. You can type in security risk assessment tool HHS. It will be the first hit that comes up on your search engine.

Valerie Watzlaf: That is the thing. There are so many resources. I love the SRA tool. I have used that. I

was just sitting here thinking, what do we do. What can you do really to get it to improve?

Ask a follow-up question. Do you see those some that do improve, they do improve over time as you go back and look at them?

Tim Noonan: Yes. There have been some instances. It is a limited field, so I do not know that it is statistically significant to say they are being responsive to the technical assistance. A handful of instances that we have come back through a new triggering event, and we have seen it. There are entities that do that. I do not know. Maybe we have to start publishing testimonials on the security risk assessment tool website like yourself. The most fun I have had this year – the greatest thing I have ever used.

Valerie Watzlaf: I could do that. Thank you.

Melissa Goldstein: Denise Chrysler.

Denise Chrysler: I was thinking about all the resources that are available and yet getting questions about could you create resources. I am wondering if it is the situation like the studies if you have a choice of buying 16 bottles, different flavors of jelly or jam. You walk outside the store because it is so overwhelming. You do not know where to begin and you cannot make choices. And with me, just thinking of my small little office and what are the basics we have done or not done. You think it is also complicated that you throw up your hands and you do not even want to start. I am just wondering if there is a way to curate and I know – it sounds like resources are divided by who they are most useful to, but sort of the security 101 for those who thought security was not for them as a starting place for small offices like my own and going from there.

Tim Noonan: That is a great observation. One of the things we did a few years ago – it actually started with one of our regional offices, the Denver Regional Office. Give them some credit – is a targeted outreach to small providers. They came up with it. We love the idea. We implemented it OCR wide. There is a small provider deck that we update every month and that is used in outreach to these smaller providers like dental offices and solo practitioners and the folks that do not have the same resources. It can be someone in a rural setting that does not have the same access to things that are in a more city environment.

It could be sole practitioners that just have not been kept up to date. They do not have an IT officer. The privacy officer is themselves and they are not even aware of it. We have used this deck. It really is an education 101 on HIPAA compliance. We have used to great effect across the country. Those types of outreach presentations occur every week. We are certainly open to other ideas, but your observation is spot on. We identify that too.

It is the smaller providers that have the harder problem. The bigger entities have the resources. Sometimes it is a decision, or it might be something – the CFO and the privacy officer have to have a meeting of the minds as to what they are going to spend on their budget. It is the small folks that sometimes do not have anything in place and they need the most help and we do that. Great thought.

Julie Chua: If I can add to what the 405(d) is also doing. We focus on small-medium. There was a year

also that we focused on the rural settings and reaching state departments. We were successful in a way where we had some engagement with specific states. And there is one state that is pretty much amplifying what they learned from us. They themselves – the states – helping human services. They are implementing, looking at the HICP, using those resources and then now they are kind of doing their own local education, using the same materials. That is always good to hear that that is an effective way for HHS to get out and provide that for the more localized engagement.

The pandemic hit. It was really a pause in terms of us being able to go to different states, doing town halls. The reason why I amplified that those that town halls are effective is we only did two engagements with that state. And then doing everything that we would never be able to do with the resources that HHS has. Basically, they are the ones now taking the charge, leading it within their states, and making sure that their other constituencies and communities know that these resources are available.

The other side of things is the past group has also put forth different types of resources, depending on the rule. There are executive cards that they have produced where it is an executive audience of your board of directors, C suite. This is what you should be paying attention to. This is why you should know the HICP exists and why your team should be using it.

On the flip side of things, there is IT cards where it is your implementers, your operational teams. This is where you go where you do not want the fluff. You just want to know how to implement certain security practices.

I think, Denise, to your point, the last thing we are going to say about consolidating, collating, 405(d) also does that in terms of our series called have you heard where you put together federal agency existing resources, including OCR. We work with OCR a lot. I can never say enough of that partnership. But we collate those. FBI, DHS, CISA, OCR, ONC. Put it all together and we bucket into or categorize it into a topic. Ransomware, for example. They have one place to look at and see all the resources on ransomware. We are trying to produce more of that kind of awareness resource, and we hope to produce more, but that is definitely something we do already.

Melissa Goldstein: Thanks very much.

Tammy.

Tammy Banks: Thank you. Just a couple of questions on – I think it was slide 22 where you showed the percentage of the audits, the voluntary audits that you went out and did the first six months of the year. How many organizations did you audit and what were they comprised of? Was it targeted to small organizations only? Was it spread? Could you give a little bit more demographics on that?

Tim Noonan: Give me a minute. The short answer is yes. I can answer that. There are about 200 entities. It was split up 166 covered entities and then 41 business associates. Within that – we did an industry report that goes into greater detail so 90 percent of the audited covered entities were health care providers, 9 percent were health plans, and 1 percent were clearinghouses.

Within the health care providers, practitioners were 55 percent, pharmacies 18 percent, hospitals 17

percent, and then health systems, skilled nursing facilities, elder care. Those were smaller percentages.

There is some granular detail in the industry report. We published that in December of last year. If you go through that, it is a great read. It took us a long time to write it. That will help explain just how we did it. We did want to make sure we covered a wide spectrum of the industry. It is so huge.

The challenges of a solo dental provider versus a multi-billion-dollar, a multi-state health plan is so distinct and different that we have to include them in the same bucket when we are doing it, otherwise, we are not providing full coverage of the industry.

Tammy Banks: Did you see any impact – two-part question – impact on those who had the HITECH certification, EHNAC certification, all those with the security component. Did you see more compliance, more ones and twos that have gone through that process or is it just still across the board? Because there are so many different security certifications right now. Unfortunately, some entities have to do three or four or five in order to satisfy their partners so to speak. I just wondered if there were better scores. Is there any direct impact? Because on the fines list, I saw some on there that have gone through compliance security analysis, and I am just kind of surprised.

Tim Noonan: I cannot say with specificity. It has just been too long. I would have to go through that. I do not want to hazard a guess. I am sorry.

Tammy Banks: No worries. Thank you.

Melissa Goldstein: Jacki, go ahead.

Jacki Monson: This might be an unfair question, but I am going to ask it anyway. Some of the earlier panelists – we were having lots of conversation, not only about third party, but like a C technology, and a couple of different themes that we heard is the idea of potentially incentivizing covered entities or essentially organizations that have this legacy technology to phase it out at a more rapid piece than they would necessarily do today because it is too costly to be able to do it.

I am curious what your thoughts are on that and if you have other ideas beyond incentives to sort of deal with the legacy technology issue that we have biomed devices that you cannot even put multi-factor authentication on to be able to solve it.

Tim Noonan: Sure. Legacy systems present an interesting challenge. When a software vendor decides to no longer support a product that can quickly cause it to be out of date. You are not able to implement all the necessary security items, et cetera. It is an area of interest for OCR.

I do not have a whole lot to say in terms of incentivizing the industry because I think there are reasons why you might maintain a system, a legacy system. There is some value or the cost to replace them are too high. There are things that can be done to limit the impact, who has access to the system, whether it is connected to your entire information system or whether it is separate, things to minimize the risk when security functions are not as standard as everything else is. I would be interested in hearing more.

It was brought up earlier, the recognized security practices amendment to HITECH. That creates a bit of

an incentive for entities to implement that recognized security practices and use them at a mitigating factor for us to consider when we are looking at imposing a penalty or informal resolution or even winding up an audit. It is still too early to see what the results of that is going to be. That just came into law in January.

Coming up with more mechanisms so it is not just HIPAA enforcement and the stick, but the other way of incentivizing entities to really catch up on their responsibilities is something OCR would support. It would be interesting to further discussions or further analysis.

Melissa Goldstein: Thank you and thank you from all of us to both our panelists for being so generous with your time and knowledge today. We really appreciate you coming and talking with us today as we think about how we could move forward on these issues. Please let us know if there is anything that you think of that we should follow up on after the fact.

I think according to the agenda, we move to public comments now, Rebecca.

Public Comment

Rebecca Hines: We do. Yes. Thank you. For those of you who are with us live right now, if you would like to make a comment to the committee, the instructions are here. You can raise your hand, to have your audio unmuted or go into the Q&A box. If you have called in, you can press *9. I just checked the NCVHS mailbox and did not see anything. I did want to make you all aware that on the website, we did receive – they have posted the two comments that we did receive. Hopefully, you can see those. They are on this page that I just put into the chat at the bottom. There are two comments that were sent, two written comments.

Greg, do we have any live comments coming in?

Greg Richey: Nothing so far.

Rebecca Hines: I will check the email one more time. Greg, do you want to just review the process for making a comment?

Greg Richey: Sure. If you would like to make public comment, you can use the raise hand feature to indicate that you would like to make a verbal comment. You will see a raise hand button at the bottom middle of your screen, similar to where the mute button would be if you are in a speaking role. If you are on the phone, you can press *9 to raise your hands. If you do either of these, we will be able to call on and you will be able to make a verbal comment. If you would like to make a text comment, you can also use the Q&A box, which is also located at the bottom of your screen. Simply type into the Q&A box your question or comments and it will be read out.

Rebecca Hines: Let us give folks a moment to see if we hear from anyone. It does not appear we have any public comment at this moment. If someone is delayed, we will keep an eye out for the Q&A. But otherwise, I think public comment is closed unless we hear from someone in the next few minutes who was not able to get in for some reason.

Let me turn it back over to our co-chairs.

Jacki Monson: I do not see Melissa, but I think we just want to thank everybody for all of your participation today. I know that I learned a lot as a very robust discussion. I think we have a lot as a subcommittee to discuss what next steps are and what would be helpful. I think today was both terrifying and interesting all at the same time and just reinforces why I do not sleep at night. Looking forward to seeing what we can do to create some recommendations for the secretary.

Subcommittee Discussion: Review Themes, Identify Potential Recommendations and Additional Information Needs

Melissa Goldstein: Agree. I believe we have some time now for subcommittee discussion. Rebecca, is that correct?

Rebecca Hines: You definitely have up to an hour if you want it to summarize. You have scheduled up to an hour. You certainly do not have to stay on for an hour. It is good while things are fresh to just put out there so we can take notes for follow up.

Melissa Goldstein: Okay. Thanks. Jacki, Denise, Val, anything to put out there right now?

Denise Chrysler: Nothing from Denise.

Valerie Watzlaf: I have taken so many notes. I have a long list of the themes that we were hearing today. There are so many. But I think some of them are just the partnership part I think just making sure that there is much more collaboration even with government and with others and even when you go ahead, and you are putting out many of these resources to improve that.

So much about solutions, I think, just making sure that there are easy solutions, which I do not know if those truly exist, but that make a playbook, something that would be easier to implement particularly for the smaller facilities.

Those were some of the things that I think just kept hearing today as well as – leadership, I think, is something that is important too. It really has to start with the leadership with the different organizations and all of the work around prevention with risk management and risk analysis and so forth. But I have more, but I will be quiet and let other people speak.

Melissa Goldstein: In terms of the legal structure, it has been interesting to me to hear today about the various mechanisms that already exist and the need to get them moving and the work and time that it takes and that it will take to take advantage of the mechanisms that exist and that it is not necessarily that we need new statutes. I understand there are regulatory processes going on and that we all wish that regulation happened faster than it does. Those of us who have worked on making it happen understand that it takes a lot of time and effort to get them out there along with process that is required by law.

There seems to be increasing effort and a bunch of different groups that are working on moving this forward is what we can do as a committee to accelerate, amplify, help, investigate, look into it, to see

how we might ease some of these processes. Perhaps be a lubricant for the wheels that have to move forward and how maybe we could convene, maybe we could see what recommendations we could make.

Particularly, it was interesting for me to hear the opposing views of OCR as an enforcement agency and full of penalties versus the idea that we just heard Timothy Noonan talking about wishing that there were incentives, prevention methods, the ideas about the education function and the webinars, and it's almost like we need a set of navigators from the federal government that are here to help, right? Here, get you up to speed so that you're not making the C or the D.

Of course, as an academic, I'm drawn to these grading scales. Like, how do we help you? Who are the tutors? How could we help you get up to speed so that you're not risking making the D, you're not risking being called out next time around.

So these are some of the thoughts that I've had today, although they're still somewhat unformed.

Rebecca Hines: Yes, Melissa, somebody this morning said enforcement versus counseling. You know, the two different sort of approaches to this, or directing penalties towards actually remediating rather than paying to the government. Sort of somehow enforcing that the penalties are used by the organization to strengthen themselves.

Rachel Seeger: So to Melissa's, I was hired following the HITECH Act to lead public affairs and outreach for OCR, outreach to the industry and to lead a national campaign between OCR and ONC to increase awareness of health IT, privacy, and security, not only among the healthcare industry, but among consumers, and this is an area that is just really not well-funded. OCR will tell you that my FTE is split between HIPAA now and the rest of OCR, and part of my FTE is spent with you all.

I'm the only person doing communications for all of us here. So when Tim talked about the cybersecurity newsletter that went out today, I posted it on the website while we were in the middle of this hearing, with everything else I was sending to all of you, and I disseminated it on the listserv. I haven't tweeted it yet, because I haven't had the time.

But we don't have enough investigators to handle all of the complaints that we receive and all of the breach notifications. Tim said we have to funnel it down to what will be most impactful, and I think there's been some question and discussion would it be more impactful to hire more people to do outreach, and that is a question for all of you. But you're right in that I do think that the mechanisms already exist. Tim talked about the fact that the statutory authority is sufficient with respect to enforcement, and the issue that we're seeing is that we've always said, and this is picks up on what Val was saying earlier, leadership sets the tone. It really is the C suite down and creating a culture of compliance.

And we had a representative from C suite join us this morning, John. He was with us in the capacity of a learner, and he said to me, he tweeted to me or sent me a private message: the landscape seems reactive with limited ability to apprehend. As with my kids, if there are no consequences, the behavior won't change. The threat actors will continue to pillage. He also said to me, this is an area he doesn't know very well, which I think is really telling, given that he is the CEO of a covered entity. No matter

what the size and scope of that covered entity is.

And Jacki, you and I have had many conversations amongst ourselves about the challenges of not only compliance but also IT, which is getting the resources needed and getting heard in terms of getting in front of the board, in front of the C suite, whomever it may be.

And I think that the conversation that we heard this morning from UCSF and Sonoma Valley Hospital was really telling, if you look at that slide about how many FTEs they have working for them and what their budget is in order to handle IT and security. I sent that slide deck around to my colleagues, leadership within OCR.

First of all, you have to commend them for their candor in coming before this hearing and talking to all of you in a public forum about what they're dealing with, but that slide about how under-resourced they are is just really telling.

Jacki Monson: So, back in 2017, 2016, I was a part of the cybersecurity taskforce which was tasked by HHS and things have not changed. If we went back to those recommendations, a couple of them have carried through. The Healthcare Sector Coordinating Council, which Erik was talking about, Erik Decker was talking about this morning, has tried to make more meaningful progress, but the reality is the problem has actually just gotten worse, because healthcare is just even more targeted than it was in 2017 and 2016.

So that's obviously from my vantagepoint deeply concerning, and I think you've accurately articulated the problem, and even the big health systems are impacted. I had to reduce my FTE count by more than 60 because of the COVID pandemic. So I'm faced with the same things that the small organizations are is what are we going to spend our time doing, and when you look at major security initiatives like let's just take network segmentation, which is a way that you would possibly prevent those legacy technologies from infiltrating your electronic health record, it's multimillions of dollars because of the way that healthcare was built and the way that it grew up in the subspecialty area.

And so I truly believe and I think we heard that from our panelists this morning, especially Denise Anderson from the Health ISAC, her comparison to the financial sector is the problem of what we're facing because of how we sort of grew up as a healthcare ecosystem has made it ten times worse, and we don't have the same problems that the financial sector does in the sense that they have streamlined technology, they don't have legacy biomed devices, and even though I feel very supported by my leadership team at Sutter and I think if you met the CEO that I work for, I think she would tell you a lot about privacy and security and all of the phishing campaigns that she doesn't click.

But that doesn't mean that the CEO isn't having to make difficult decisions based on risk about what we're going to do or not do, and when you have legacy technology that's really expensive to replace, it's a tough conversation to have and most of that stuff doesn't even include something like multifactor authentication.

So I think that was sort of my observation from today, and I think there's a lot that we can amplify based on things that even the taskforce had evaluated, like for example the idea of incentives, they had actually, we had proposed for lack of a better term sort of the cash for clunkers program for technology.

You trade in your old technology, you get new technology, and as a result of that, you get some kind of an incentive, and that's one of those recommendations that really didn't go anywhere, because I'm sure it's hard to figure out, well, where does that go and where does that belong and how would that even work?

But I think there's lots of opportunities like that to amplify some of that. I think the threat intelligence sharing is pretty significant, and a few years ago, there was lots of conversations about, well, could we potentially get people to have security clearance so that they could obtain this intelligence information and there really hasn't been a process or protocol created for that, but I think getting that information in real time so that we're not in defensive mode and that we're in proactive mode is really helpful.

So I think there's lots of good recommendations that we heard today that at a minimum we could amplify in our letter to the Secretary, and I think I just continue to think about, you know, we've made some progress, but we haven't made progress fast enough and what I fear while we are in the middle of not making enough progress quick enough is this impacts patients and it impacts their lives.

At what point do we just say enough, because it impacts the safety of a patient and could actually cause death? So that's sort of the lens that I look at this through and that's why I stay up at night and that's why I spend as much time and energy as I do, both on this committee as well as in my day job, trying to fix as much as I can from a security standpoint, but the reality is everybody should be thinking about it in that same way.

Melissa Goldstein: Anybody else want to make preliminary comments, reactions?

I just wanted to check in with Nick, if he's with us, just to make sure. Our chair.

Nick Coussoule: I'm still here. No, I'm really with Jacki a lot on the things that she was just talking about. I have the same accountability in my role. I should say I have the security function, information security, all as part of my responsibilities and has been for about a dozen years. So I live this every day. So no, I'm actually kind of fully in line with what Jacki was just talking about, some of the challenges.

Rebecca Hines: I just want to remind the members that Vickie shared some thoughts about potentially academic medical centers working with smaller hospitals and federally qualified health centers to help with cybersecurity threats and also looking at ways to take a preventive stance more than responding once the bad events has happened. So just thinking about prevention and the ecosystem. So just a few thoughts that she put forward for consideration.

One thing that might be helpful just from a strategic vantage is once the transcript is out, we could just quickly pull out each of the moderators really adeptly asked the speakers what would you recommend, that we recommend, so we could just pull that out in a laundry list of, okay, here's what the speakers said were the top points. So that would be one starting point.

Maya Bernstein: Natalie and I have been taking notes all day, and I haven't been able to pay attention 100 percent the whole day and Natalie had to go on training for the middle of the day, but we have a lot of that. So I don't know that we have to wait for the transcript, which usually takes a couple weeks, but we can get you some of those. We can get you some of those sort of highlights or themes or answers to

those kinds of policy questions that you guys asked, and I've been sitting here trying to pluck it out, but truthfully my brain is pretty fried at this time during the day. It's been a very long day, very productive I think, and even with all the changes in the panelists and the last minute whatever, I think the people that we did have were very engaging and I was really pleased about this came out.

I will try to early next week I guess is probably the earliest I can get to it is pull together some major themes that I heard. I obviously thought melissa's comments were very interesting. I wasn't thinking about it sort of the way she heard it, that she just described sort of a legal matter how do you actually implement this stuff that's already in place, was an interesting way that I haven't been thinking about it, I've just been sort of linearly taking down whatever I can.

So when Natalie and I can put our heads together and just try to give you a jumping off point for things that we heard and then we can continue the discussion from there. I am not sure when our next meeting is, but somebody will tell us. But if there's other themes or things you want us to capture now that are particularly stuck in your mind from the day, I'm happy to try to just take note of them.

Melissa Goldstein: You just made me think of another thing, Maya, thank you. So other than the RFI and the NPRM that Erik Decker was talking about, I believe the only other possible legal change that we heard -- and please correct me if you guys remember wrong, but we'll also check with the summaries -- was Tim Noonan talking about the new enforcement penalties that were set and the stages and the limitations in HITECH versus the original regulation. And those would need to be changed if we were going to change them, but that makes me think about this idea of is it the number, the amount of the penalty that is going to change an organization's behavior? An after the fact punishment, which is the purpose of a penalty, right?

Or is it some other action along the way or is it the fact of the penalty itself and the publication of a penalty? Is it the size of a penalty? What is it that matters? And is the penalty itself going to make the difference? Is it whether it's $6 million or $8 million or $10 million, if we look at the Anthem numbers, which is an interesting question for me, like, would that be the right focus of energies right now, or is it some other focus?

Sorry, Maya, I cut you off.

Maya Bernstein: No, no, you were still speaking. No, just responding to that, imagine -- I am thinking about the story about how Steve Jobs didn't like having a license plate on his car. He thought it was aesthetically not pleasing. So every time he got stopped, he just paid the fine, because it was a few hundred bucks and he could afford it, right?

So that's the kind of thing we're talking about with an organization as large as Anthem or something. At some point, the amount of money does matter. At some point, it's too small and it's just a cost of doing business to allow me to keep violating or flouting the law, because it doesn't cost me enough to actually fix it, and at some point, maybe it's too much or whatever, but I do think there is something about the amount of the penalty that makes a big difference for a small entity and the same amount is nothing for a very big entity. It's sort of in the noise and in the cost of doing business.

And there's maybe a fairness issue there about whether you can have what we know to be several-

hundred-million-dollar kind of penalty for Anthem that's in the private sector versus whatever settlement they came up with, which was much, much smaller from OCR. So I think just to respond to that particular point, I think there's something to that. However, I agree that there's many other things we heard today about what we could do as a government to incentivize people or help people or bring people along, or whether it's to provide training or technical assistance or cajoling or make the documentation or the kind of where NIST was talking about they have these long thick technical reports. I'm definitely, every time I see one of those review, I'm like I'm not digging into that.

But they're trying to put it in more digestible forms for different kinds of audiences so that we can talk to the CEO who isn't really an expert and make them -- you know, encourage them to understand why this is important not just to their bottom line but to their mission and so forth.

So I think the strategy -- and this is of course just me talking off the top of my head -- but the strategy would be kind of multifactor, right? You want to have penalties, but you also want to have a way to provide, be the teacher so the student doesn't get the C or the D, right? Provide ways to bring those entities along that will allow them to do better in this environment, essentially.

Nick Coussoule: Maya, I think that's a really good point. I didn't mean to interrupt, but both the carrot and the stick are necessary in that model. Now, the actual financial amount may or may not be significant to somebody like an Anthem, for lack of a better term, but there's also reputational risk, potential client defections, trust that you gain in the marketplace. So there are a lot of things that come along with that kind of a public report that are beyond just what I'll call the immediate financial result.

But I do think that the other side of that, and I think we got a lot of that discussion in regards to NIST earlier, is the point of this is less about punishment and more about education and helping people get better and doing those things. So again, I think you want to make sure that what I'll call the bad apples, who really aren't doing the right things and aren't trying to do it, to encourage them to do it. At the same time, what kind of capabilities or resources can we apply to help people that are trying that may just not have the resources or the skills or the capabilities.

So I think there are necessities for both of those, but I think the second piece of that which is the help, education, that is a much broader challenge across the industry, because it gets into the smaller players that don't have the same resources that some of us -- I got 150 people on a security team. People that don't have those kinds of resources can't do these kind of things the same way. So I think that's a really, really helpful one in the way that the gentleman from NIST framed it up earlier.

Jacki Monson: I think also just the whole leadership comment that I think it was Val who brought that up earlier. I recently, I take calls from any CISO any time of the day, because if they need my help, I'm happy to help, and one of the most recent cyberattacks I took a phone call from that CISO after they'd been down for five days, and it was a lot of expression of frustration and that I'd been trying to get approval, trying to get approval, for all these things that I thought we needed, and I couldn't get approval.

So I think that plays into it, and it could perhaps be the way they delivered it, but at the same time we can't spend all of our time and energy when we're in delegated authority positions trying to convince

senior leadership that this is something they need to invest in. So I think that's an important component of the education is sort of how do we get to that C suite group to understand the importance of it equally to the small practices, because I'll give an example: I was jumping up and down very excited when we got the Stark and Anti-Kickback exception, which would allow us to provide almost 2,000 independent physicians with cybersecurity technology, and they're interconnected with us in all that they do.

I thought they would be thrilled that we would be covering the cost of the cybersecurity technology and I thought we would in a couple of months be able to deploy it, and it was like a sales campaign for the first six months to try to get them convinced to deploy -- to take the time to deploy the technology. But I will say now that we've actually proactively prevented things and are providing the reports to them of the things that we've saved them from, the downtime, the potential patient trust issues, it's a whole different ballgame and conversation.

So I do think it's related to the message delivery, but I just share those two experiences as part of what our panelists were trying to articulate this morning especially and the challenges that they're faced with.

Rachel Seeger: So one interesting wrinkle in this is the rise in cybersecurity insurance or breach insurance. I do not propose this to you as an area that we would look at, because the hearing was focusing more on security in general, not cyber, but with cybersecurity insurance, maybe there's less of an incentive to do the work, because the insurance is going to cover organization in the event of a breach. Now, it won't address the reputational harm that Nick was speaking to, but with respect to any type of other legal remedies, other issues, the insurance might cover that.

Jacki Monson: That's a good point. I think one comment, one interesting thing, Rachel, on the cyber insurance. So premiums are estimated to be increased by 134 percent this year for all organizations who are impacted. So the trend that we're now seeing in negotiations, and these are large significant multibillion-dollar vendors that we are doing business with, have now written into their business associate agreement, because normally we would have provisions require them to have some level of cyber insurance, that if it's not affordable, that they will not carry cyber insurance in that negotiation, and that has evolved over the last probably six to eight months because of the cyber insurance premiums increasing by 134 percent.

Cyber insurance renewals, for those of you who don't know, they are updated every year. You can never get a multiyear plan, because they want to obviously be able to look at the data, and this is still pretty new territory for insurance companies. But because of the cyber-attacks, the premiums are going up by 134 percent, I can tell you that even an organization like mine, we're going to be taking a hard look at whether we can afford cyber insurance if it's really going up by that amount and what's that worth.

So I think that's another wrinkle with the cyber insurance piece that is challenging. The other area, Rachel, that I'll just mention relevant to what you were just talking about is something that I don't think came up in the hearing but has been interesting. A lot of the medical malpractice insurance now that small physician practices have to carry require them to have some level of cyber insurance and to provide now some level of certification and assurance that they have basic minimums of a security

program. And that's just evolved over the last year or so, and I think that's just an interesting concept.

Melissa Goldstein: I'm not familiar with I guess the legal structure of the contracts with the insurers, but I'm wondering if there are exclusions for, say, negligent actions on behalf of the company or lack to conduct a risk assessment, lack to have an enterprise risk assessment, ways that the insurance company doesn't have to pay if the organization itself is not compliant with requirements under the law, things like that. This is just off the top of my head. It would be an interesting thing to look.

Jacki Monson: There is. I think it varies across the board depending on probably the level of risk you are when the underwriters are evaluating, but things like if you pay ransomware, then your cyber insurance would cover; if you actually violated the HIPAA security rule, things wouldn't cover. So there's quite a few provisions that I've seen in the 20 years I've been in this field, and they just keep getting more robust and keep excluding more as I think the underwriters and the insurance companies get smarter about what they can insure and what they can't insure. But there's quite a bit of exclusionary language in the tune of close to 1,000 pages when you get these types of agreements to enter into insurance.

Melissa Goldstein: I'm smiling because it's a way of privately enforcing the laws, right? The HIPAA security rules.

Jacki Monson: Yes, it would help if it was affordable, right? If it's you gotta pay 134 percent premium, that's just, that's going to be hugely challenging for a lot of organizations, and I think the billion-dollar companies, they saw this coming before everybody else did, because they started writing into their business associate agreements late last year, and at least from my vantagepoint, I was questioning, well, why would they include that provision? That's crazy. Why wouldn't they have cyber insurance? And then you realize that premiums are going to go up to that level, you're going to have to make some tough decisions, because people aren't going to be able to afford those premiums, and/or they're just too much risk.

Maya Bernstein: I think Rachel's right that the incentive structure is changing and that's very interesting, but at some point, if the price goes up high enough, maybe it's cheaper to actually invest in your damn security, right? Like if you had all those things in place, then you wouldn't be so worried about the insurance.

I think, Melissa, most of the time insurance covers negligence. That's what it's supposed to cover. Like you think about a car accident or something, it's covering negligence. It doesn't cover, like, willful violations. Often there's exclusions for that. But this is a new area of insurance. You gotta wonder what they're going to come up with, and in terms of who's paying, as Jacki was talking, who's paying and which side of the covered entity is this associate agreement for whose fault it is between those two entities and so forth. It's kind of interesting.

Melissa Goldstein: And to Vickie's point, which Rebecca mentioned about the spectrum of organizations and those small and medium providers or the community hospitals, the ones that are so underfunded to begin with, insurance certainly with the premiums that they are now is not even an option.

Nick Coussoule: I mean, insurance is basically risk management, right? So you're always making a weighted decision as to do I buy insurance or do I self-insure, and in either of those circumstances, then

you talk about what investment do I make to mitigate those risks? So it's like a three-dimensional chess game. It's not a simple buy or not buy, invest or not invest. You try to weigh out all three of those components and then decide where do I spend my money as an entity, and when you start talking about am I going to go this or am I going to invest in other equipment to help patient care, do other kind of things, it's a very difficult, not a trivial decision process at all.

Maya Bernstein: Right, although of course insurance is after the fact. It's not going to bring back records that are lost. It can compensate you for certain kinds of things, but there's certain things it just can't fix, and so there's a balance between how much you're investing in your security posture, as Nick was saying, or on buying a new MRI. There's a lot of different factors in the kind of limited resources that we have heard about all day.

Rachel Seeger: Another piece of this is the rise in class action lawsuits as a result of these breaches, which I see Jacki shaking her head affirmatively. They have risen exponentially as a result of these ransomware attacks, like crazy. While some of the class action lawsuits may only have two people who are part of the original action or suit, you also have the state attorneys general coming into play.

Nick Coussoule: I do think it's that the change in the rules to focus on somewhat of a mitigation, if people have demonstrated good practices as opposed to the -- it's kind of like they're penalizing the people that got robbed instead of the robbers. I think that's a good step in the right direction of recognizing that also there's somewhat of a -- if you do the right things, there's some limited amount of risk in a lot of different ways, including that regulatory perspective. So I think that's a very positive change as well, which I'm not sure if it was Tim or somebody else highlighted earlier today.

Melissa Goldstein: I think we've got a lot to talk about in our next subcommittee meeting. Thank you all. Thanks very much for everybody's time today.

Jacki?

Jacki Monson: I just appreciate everybody's time today, and I agree that we have a lot of opportunities to chat about and I think we have subcommittee meeting next week. So it should be a very robust discussion.

Rebecca Hines: Very good. So let me turn it over to our chair. Are we ready to adjourn?

Nick Coussoule: I think that's what I heard Melissa and Jacki saying.

Maya Bernstein: I do want to take some time to thank the staff. I don't mean me and Rachel, but Rebecca and her staff, Geneva, Marietta, the contractor staff that have helped us put this together.

Rebecca Hines: Really, as those of you who've been on email for the last 48 hours, you know that this is team sport and without the contractor, without Marietta and Geneva, this meeting wouldn't have been made possible. So just a real hearty round of thanks and gratitude. I just want to say our contractor is incredibly flexible with updating six versions of the agenda and so forth.

Rachel Seeger: Greg, Kim, thank you for everything, Bethany, all of you. Thank you for being so

responsive throughout the day with updates to the website, updates to the agenda, updates to slide decks that we were receiving. You are the best, as always.

Maya Bernstein: And despite all of the bobbles with the various panelists in and out and whatever, I think Rachel really put together an amazing program for us today and a lot of kudos to her for all the work she did to get us to this point.

Melissa Goldstein: Yes, thank you. You've made our job much easier, which we really appreciate.

Rebecca Hines: All right, let's adjourn for the day.

Nick Coussoule: We're officially adjourned. Thanks, everybody.

(Whereupon, the meeting was adjourned.)