Tim Rahschulte:

Well, hello everybody. I hope you're enjoying this event from GovExec. It's no more important of a topic than cybersecurity, and what I'd like to do is spend a little bit of time with you and talk about cybersecurity in terms of being a team sport. A lot of times we hear the need to constantly do more with less, the need to align competing priorities, the need to think about how we manage the limited resources we have with the multitude of projects that are in front of us and the way that we do that, the only way that we can do that is through collaboration. Collaboration, first and foremost inside our organization and then among the partners that we work with, think of our suppliers and our vendors. These are partners to help us best defend, prepare, and respond to cyber threats as we see them on the landscape that we all participate on.

And that's the reason that cybersecurity is a team sport and that's what I really want to spend a little bit of time speaking with you about here over the next, say, 30 minutes or so. My name is Tim Rahschulte and I am an executive vice president here at GovExec and I am the co-founder of the Professional Development Academy, the organization within GovExec that delivers cybersecurity simulations as well as cybersecurity leadership training programs, and I'm going to talk a little bit about that later on in this program and give you an opportunity to participate free of charge in our quarterly simulation, which is the next one is coming up in June.

So, more of that coming up here later in the programming, but so far within this event, you have covered a lot of content relative to the landscape of cybersecurity and no doubt whether you're a high level leader within your agency, if you're within IT, maybe you're specifically within a risk area, risk manager within your agency and focus solely on cybersecurity. Maybe cybersecurity is one of many hats that you might wear within your agency. Maybe you're not on the IT side, maybe you're on the procurement side and you're involved with making sure that you have the best tools available, whether it be software tools or training tools to make sure that your workforce is ready and resilient when it comes to addressing the world of threats that are around us.

Again, the content you've covered so far has really painted the picture of the landscape, and that's what this slide really focuses on as well. It wasn't too terribly long ago. Think a few decades. Relatively speaking, that's not a lot of time, but a few decades ago, we were focused pretty much in that mid-section of this world of threats. We were worried about physical challenges of our equipment, of our offices, of our infrastructure, the way in which we carried out our work. We were concerned about fires and if we were in certain flood-prone areas, we were concerned about floods. Same thing with hurricanes or tornadoes. Those are more prevalent and carry a higher level of risk in some geographies of our country as compared to others.

Earthquake's the same way. Pandemic's the same way. What happens if these disasters hit our organization, our agency? What is our disaster recovery plan? What is our business continuity plan? How will we sustain the level of business that our customers, those within our communities so desperately need? Over the years that have come since those times, when it was really focused on the security of physical infrastructure, more and more data infrastructure, cloud computing in these days, the more modern age as we're in right now and a whole host of other things, and I was going to say every year, but it seems like every day there's new threats, new threat vectors, new coordinated type of attacks that are coming about and we're susceptible to those and how do we defend against those?

How do we build a sense of resiliency around that and how do we make sure that we are continually vigilant when it comes to these ever-increasing areas of threat? Some of these you might be looking at here on screen saying, "I think we're pretty well-prepared for that." Some you might say, "I don't think we're prepared at all for those," and depending on the type of threat, you might find yourself in an increasing or a decreasing level of maturity and overall readiness, and again, this is where cybersecurity

being a team sport is really important. Within the GovExec Leadership Academy, we focus on cybersecurity for those that we serve. We do a lot of work at the local government level. We serve a lot of the 19,450 cities across the country. We serve nearly two thirds of all of the 3,069 counties, boroughs and parishes across the country, and we provide leadership development training specifically for cybersecurity as well as our cybersecurity simulations because we know that when we are all better prepared, the country is better prepared.

So, when we think about strengthening cities, we strengthen counties and when we think about strengthening counties, we strengthen states and when we strengthen our states, we can strengthen the entire country and that's really what we're focused on doing, and the way in which we do that is through collaboration. How do we make sure that if one county doesn't feel as if they're prepared as much as another county, how do we help bridge the gap and bring those counties together to share best practices? We say "best practices," because what's best practice now isn't necessarily best practice tomorrow, and it may not necessarily be best practice for all counties, all cities, all federal agencies. We have to understand what is best for our organization, our agency, our county, our city, our state, and what we're trying to attempt to do, not just for our purposes, for those that we serve within our area, but then how we actually coordinate that across states, across federal agencies and so forth.

So, collaboration is the key to our success, and therefore cybersecurity is definitely a team sport, and we'll talk more about that as we move through. As we move through, let's take a step back. Let's do a quick simulation and again, you might be a high level individual, high level leader within your agency. You might be on their procurement side. You might be on the IT side. You might be solely responsible for cybersecurity within your organization. You might be a program manager carrying out various projects and programs within your agency. Here's the scenario. Put yourself in the receiving end of an emergency call from your Director of IT who just informed you that some of the most critical data servers that you have at your agency have been breached along with your customer-facing website as well as the email that you use for your agency.

All of these have been breached and now, you're getting this call from your IT director and you're now being held ransom and the question becomes... Just think about this scenario. This may have happened to you already and you're like, "You know what? We learned from this in the past and we know this situation all too well." Some of you might be thinking, "You know what? What would we have that anyone would not want to hold us ransom for?" The reality is you'd be surprised. You'd be surprised what you have and the data that you've got and for others of you, you are involved in these type of tabletop exercises, these simulations on a regular basis. This is the situation.

Now the question is what are the first three plays or first play, the first few plays, whatever you want to think of? What are your first actions, the first calls you make, the first plays that you're going to run that are detailed in your cyber preparedness defense playbook, your disaster recovery playbook, your business continuity playbook? You might call it by different things, but it has a series of things that you do, these actions. Think of it as a playbook. These are plays that you're going to run to. In this case, you're already being held ransom or you're being told that you're being held ransom. What are the first three things you're going to do? You're on the call right now with this individual, your Director of IT, who is telling you this scenario. What are the first things you do? Maybe the first questions you ask, what are the first actions you give to your Director of IT? What are the first calls that you now make in your role?

For some of you, you know exactly. It's like I do this, A, B, C. For others, you might be wondering, it's like, "What would I do if this was to happen to us?" And for others, yet you might say, "Well, the Director of IT is the one calling me. Shouldn't the Director of IT know what these plays are?" And yes, probably so, but you probably need to know as well whether you're a program manager in your organization or you're chief administrative officer in your organization. You want to know who's who, what's what,

where's where. You know want to know all of the details, especially when it comes to something of this magnitude, this level of challenge because this is a big challenge. This is a big issue. We see it on the news all the time and again, some of you I know have fallen victim to this and have recovered from it and are more resilient because of it, but others have not yet experienced this.

They've not yet witnessed this and so we want to talk through some of these simulation examples and let's take this a little bit farther. So, you've executed the plays necessary to recover the data from the ransom. So, you've got your data back. You don't know if it's only now with you and it's no longer with the ransom holders, the people who have attacked you. They might still have this data. They probably still do if they had it in the first place, but now the question is how do you recover your brand? So, whether you're a federal agency, large federal agency operating on a global scale, whether you are a rural, very local, rural county with a few cities in it, you've got a brand and your brand has now been tarnished because you've been held ransom. How do you get this back? How do you recover your brand? How do you regain trust from the number of stakeholders that you have?

Think again about those partners that you've got, the suppliers, the vendors, the partners that are actually carrying out some of the work that you do to provide services and products to those that are in need within your communities. How do you help your community constituents? Think about the governance committees that you're a part of that you need to think about rebuilding that brand, rebuilding that trust. Community members themselves who rely on your services and products and maybe importantly of all of them, your employees. Does your playbook go through that level of processing? Our experience is that in many cases, they don't. They work to not only have we backed up our data? If we have a disaster, can we recover our data and reestablish that to continue our business operations? That's what has been focused on. That is what in many cases continues to be focused on, but more and more important becomes the brand that we have relative to the products and services that we carry out every day.

So, it's something to think about. Think about the playbooks you have in place or maybe don't have in place at this time as we go through these next several minutes here for this segment and as you continue on into this event from GovExec. As you think about this simulation, we just were held ransom. We recovered from that ransom and now we're trying to rebuild our reputation and as you think about that simulation, what is the most effective as well as the most vulnerable primitive level defense mechanism securing your data assets today? And if you want a hint that there's a single word that is the right answer to the question, that's the hint, but it's the most effective mechanism you have that's going to secure your data, the most effective defense against threats. It's also the most vulnerable and many of you already know it and already you might have a smile on your face because you know how effective it is. You also know how vulnerable it is, and it's people.

People are the perimeter. People are the perimeter of everything that is happening that's good in the services and products that we provide, those that are our customers, those that we serve every day in our cities, in our counties, across our states and across this great country. People are the reason that those great things happen. People are also people and they are vulnerable. They do continue to get these phish attacks in their email and it only requires one time that the threat actor to be right and our people to be wrong for something bad to happen, but conversely, our people have to be right all the time to defend against some of the phishing attacks, the malware attacks that we have, the ransomware attacks that we have, all the other terrible cyber attacks, simulation or cyber attack threats that we have. We can run simulation after simulation after simulation. People are still people and the phishing attacks and the threats that we see are getting much, much more sophisticated as well.

They're being much more cloaked and much more camouflaged in terms of it being a real issue, a real threat. The emails we get, the phishing attacks that we have, they look more and more real all the time.

So, we can certainly understand how in a lapse of judgment, someone clicks on that link. Someone opens up that document and unbeknownst to them maybe for a long period of time, there's malware now that is running on their system. So, how do we actually recognize the success we have with people and manage the challenges that we face on a day-to-day basis? Whenever you give a story, sometimes it's usually like, well, do you want the good news or do you want the bad news? When we provide stories especially around cybersecurity, there's sometimes the good, the bad, and then the really ugly, and then there might be some other things as well that we want to throw in, but let's just talk about the good, bad and the ugly when it comes to cybersecurity and especially cybersecurity as it relates to being a team sport.

So, the good. Let's start with the good, right? The need for cyber risk preparedness, readiness, resilience is generally well understood. It's more understood now than it was at the first of the year. It's more understood now than it was this time last year. It's way more understood now than it was just a few years ago. Our general awareness, our general understanding that we have to be vigilant, we have to be resilient is good. This is a good thing. People know to be a little bit more mindful before they click on that link. People know about the threats that we have in our organizations, in our government.

People are generally aware. This is a good thing and we don't have to look far. We can see in whether it be through Route 50 or any number of other organizations, there are a lot of outlets that will promote here's how that we can get even better ways that we can get even more vigilant, more resilient to defend against the threats of cyber attacks, and whether these are rating tools to assess our risk readiness or if it is training that we offer. GovExec, ourself, as mentioned earlier, the professional development academy that I run, we've got a lot of training. There's a lot of providers out there that provide really, really good cyber awareness training and so we're getting better and better and this is a good thing and this should be celebrated.

So, if you haven't recently celebrated some of the wins that you've had. I know we get so focused on the negative and so focused on putting out the fires and making sure that our business continuity is in place that sometimes we miss the fact that, hey, did you know that we stopped the 800 attacks over last since the first of the year that are threatening our servers? Are you aware that we infiltrated this threat actor in such a way that we were able to isolate this person or this group of people when they're trying to get to our systems? Pausing at least a little bit of time to recognize the good that the employees are doing is time well spent because it is good.

There is the bad. Threats and cyber attacks are occurring faster now than they ever have and in many cases, within many organizations, they're happening faster now than what our organizational readiness is ready to defend, and again, we can look to organizations like Route Fifty and others that there's still a number of organizations, government, as well as private industries alike that are using federally banned technology and this is something we're getting better and better at identifying and resolving, but the reality is we still are using some services, some technology that has been banned and we can do better and we are constantly working to do better.

So, if you are wondering, it's like are we one of those organizations? Maybe you are. If you're on the procurement side, have you updated your procurement rules, your regulations, your policies?

Have you updated your contracts and agreements? Have you made this known across the managerial staff who are working with you for procured items to make sure that you are in compliance with federally banned foreign technology? Are you in compliance with certain reporting protocols? Are you in compliance with certain audit and assessment protocols? These things can become known and through a number of organizations, GovExec being one of them, events like this being one of them. Again, cybersecurity is a team sport. Are we collaborating and sharing best practices? Because we can grow faster together than we can otherwise alone. We can share known information. We can share

knowledge to help us grow faster and that's what we need to be able to do and that's one of the reasons for these events such as what we're having today and virtually as well as onsite. Now, the ugly. This does get ugly.

You probably have engaged in maybe on an annual basis, semi-annual basis, you probably engage in what-if scenarios. What if this cyber attack happens? It's a similar type thing, is a simulation we just walked through. It's scenario planning. What if we do get held ransom? Are we prepared? What if we have a website defacement? Are we prepared for that? What if we have a bad actor inside the agency? Are we prepared for that? Do we have the right protocols in place? Do we have the right systems, the governance protocols, the assessments to make sure that we are as vigilant as we possibly can be? For some of you, you're saying yes. For others, you're probably saying, "I should probably find out if we are," and the ugly part of this, especially cybersecurity, is the impact is usually greater than what we expect and so let's just take two very different examples.

Let's just say somebody got onto your website and put it in falsified information. There's a website defacement that has taken place. That's a cyber attack. You might be able to work with that ISP provider and drop that site and reload a new site rather quickly and be back online, and yes, it's a big deal. It's a real issue that needs to be resolved, but the business continuity plan can be pretty straightforward and you might be back online relatively quickly without a lot of customers, maybe not a lot of customers being adversely impacted. Now, let's take the converse of that. Let's take that phishing attack that stems into a ransomware attack. Again, that phishing attack may have happened today, may have happened yesterday, last week, last month. It may have happened three years ago and someone, because again, lapse of judgment of an employee, inadvertently clicks on a link, doesn't know anything, didn't realize that anything even happened, right? Goes back to his work, goes back to her work, and a few weeks later, a few months later, a few years later, that attack starts to unfold.

The attacker has been kind of cruising the servers, looking to see what's there. They're just phishing, literally phishing to see what kind of data does this agency have, does this county have? How might I be able to use this? You may not even know that the attack happened until long after the event. Now the ugly part of this is that the lingering effect can be quite long. It's like the wake from a boat, right? The boat goes by and the wake, you see the ripples on the shore, long after that boat is gone, and the same thing can hold true with a cyber attack. Now, think about it in terms of if there is a natural disaster. Natural disaster, hurricane, earthquake, a fire, something of that nature. Clearly, there's certain things we want to have in place. We want to have good communications. We want to have good infrastructure. We want to have clean water for sanitation and for health and sanitation.

Those are three things we constantly want. The same thing holds true within our organization. Do we have good lines of communication? Do we have good infrastructure to connect that communication and enact our work? And can we sanitize and build good hygiene relative to the way in which our business operates? When there's a hurricane, a tornado, a fire, something of that nature, we might be thinking, well, the what-if scenario, right? The scenario planning. What if we're out of water for a day? It's like, okay, we can manage being out of water for a day. What if we're out of water for a few days? All right. Certainly not ideal. None of this is ideal situation. We can work by being out of water for a few days. What if we're out of water for a few weeks? Now, see, the risk starts to grow exponentially because now if we start thinking beyond just a few days to a few weeks, what if it's a month? What if it's a month and a half?

Now, the risk becomes much more dire and the probability might decrease a little bit, maybe a lot, but the impact and the risk grows significantly and we have to be ready for that. What if our systems are offline for a couple days? Okay, systems are offline for a couple days. Maybe we can put some manual processes in place to overcome that. What if they're offline for a week? What if they're offline for a

couple weeks? What about a month? What about a month and a half? What about three months? There are examples. We don't have to look far for the examples where the ransomware attack had put systems down for weeks at a time for over a month at a time. This impacts communication capabilities, infrastructure capabilities, the delivery of our products and services delivery. These become real big issues for us to contend with. That's the ugly part.

So, as you conducting your scenario planning, the takeaway here is recognize and celebrate the wins that you have. That's the good thing. The bad news is as things are happening faster than we can respond, that means we've got to collaborate more, more intentionally collaborate with others so that we can grow our defense mechanisms appropriately, and as we grow those defense mechanisms and as we think about the scenario planning, we have to extend the what-if scenario a little bit more. So, if we're typically concerned with what about it being down for a day, what about we're out of water for a week, a week and a half, two weeks? What if it's three months? Just do that one more mental exercise. What if it's out three months? What do we do? What would we do in that situation? How would we operate?

Some folks might say, "You know what? The probability is so low, we're not going to do that." That's okay. That's fine. That can be an argument somebody can make and if it's a decision made, do the best you can up until that period of time, but if it's worth another 15-minute conversation, another 30-minute conversation and another two-hour conversation to say, "What if we are out of this service for a month, two months, three months at a time?" If you've got the time to spend that extra five minutes of the mental exercise working with a team of individuals, say, "What would we do if that's the scenario you want to be in so that you can figure out the real ugly of the scenario?"

We're all very familiar with what happens when we hear a fire alarm or we pull a fire alarm ourselves. We do that because we smell smoke. We see fire. We know that there's a bad situation and everyone within earshot and an eye sight of the flashing lights, the sirens going off, the noise that's happening. We know what a fire alarm is. We all are programmed to do a certain thing. We're not programmed to collect the computer on your desk and the really important files. It's like no, you leave everything. You get up and you walk in an orderly fashion to the staircase and you get out to the safe spot and you collect inventory of who's there, who's not there, and then you start relying on your systems, calling people, working with individuals, making sure people are safe.

We all have that same level of understanding. What we want to be able to do is build that same level of understanding when it comes to cybersecurity. How do we build that same level of awareness that when we hear that fire alarm, when we see that phishing attack, how do we all have that same split second reaction that I know exactly what I need to do at this time? That's what we want to be able to try to build. The unfortunate thing is the far majority of organizations are not as prepared as they really want to be. They haven't tested through some of these threats. We all go through fire drills. We haven't all been through a ransomware drill. We haven't all been through that phishing attack turned bad, really, really bad, ugly bad and so we need to be able to better be prepared for that.

So, what I mean by that is that 20%, what we realized from that is some work that we've done, surveys that we've collected from a number, hundreds of agencies and local government organizations and officials, we know that that 20% is we've got plans in place. We've got disaster continuity, disaster recovery plans and business continuity plans in place, and they've been tested, but the far majority of them have not been, and in some cases they're not built. In some cases, they haven't been tested. This is a result from earlier this year that was conducted among counties, specifically counties that across the country and what they've said that they are optimally prepared for. Like not only do we have documented procedures, but we test them on a regular basis and we feel as if we are optimally prepared. That's the light color, the most lightest color illustration here on the bar charts.

The darker color items are those that they're minimally prepared for, not prepared at all. What happens with a zero day attack? It's about a third of the way through on the left-hand side. Zero day attack. Some folks feel as if they're pretty well-prepared for that. Many are only somewhat prepared, minimally prepared or not prepared. You can see some of the others as well. You know what? If there's someone that's subverted in the organization, very rare occurrence, but a very serious challenge and problem that we have within some agencies, especially dependent on what type of data that they might have access to. Floods and fires and hurricanes and earthquakes, we feel pretty well-prepared. The only ones who are not well-prepared are those that are typically not in one of those geographic areas that are highly prone to such occurrences of happening.

But this is an important illustration because, one, it gives us a sense as to where we're at. You could follow the same example. You could take this list from the prior slide and use this as a point of communication at one of your next meetings. You could be a high level leader within your organization. Bring this into your next IT meeting, your next risk manager meeting or meeting with managers across the agency and just say, "Just want to spend 30 minutes walking through this list and to see, do we feel as if we're really well-prepared if something bad was to happen or are we not prepared at all?" Just opening up the conversation. That's the first step in any increasing of defense and readiness is are we increasing the level of communication around the risks that we're aware of?

Even risks we may not be aware of, how do we become aware of them and can prepare for them? The other important thing to notice about this is in some cases, there are a handful of organizations that feel as if they're pretty well-prepared. Data scavenging attacks in the cloud. It's almost right in the middle of the chart here. There are a handful of organizations, a little less than 10%, eight or 9% that say, "You know what? We're not at all prepared for this." There are some though that say, "We're minimally prepared," and there are some that say, "You know what? We're somewhat prepared," and so what we do is we try to then collaborate. With those that are somewhat prepared, how do we help share some of that insight? How do we help share some of why do you feel as if you're somewhat prepared so that we can share that knowledge?

Again, this is where collaboration is the key. Cybersecurity readiness is a team sport inside organization and outside the organization. We're all trying to get better and better and better, and the way that we do that is through collaboration. So, we can look at this and pair organizations up, team organizations up. Those that do feel as if they're well-prepared or better yet optimally prepared. How do we share resources? How do we make sure that we share insights and ideas? Because no one needs to start from zero. No one needs to reinvent the wheel, so to speak when it comes to disaster recovery, business continuity planning. We can start from where someone else feels optimally prepared and then modify it based on our needs, our organizational culture and our expectations relative to the attacks and the threat probability and impact that we're going to have. The good, the bad, the ugly and the possible.

That is what's possible. Through work like this and events like what you're participating in right now, collaboration is what's possible. Collaboration is the key to our success, and so if you're at the live event right now, turn to the person next to you. Thank them for being here. Thank them for being at the event. Ask them how they're doing when it comes to cybersecurity. What are they optimally prepared for? What do they feel they're not prepared at all for? And then share back and forth with one another. Figure out how you might be able to help support one another, and if you watch them virtually, do the same thing virtually.

Pick up a neighboring agency. Pick up the phone and contact a neighboring agency or a neighboring county or a neighboring city and just connect with them. Thank them for the great work that they're doing. Recognize the great work that they're doing. Ask them what they're prepared for, what they're not prepared for, and how you might be able to collaborate with one another to move forward because

people are the perimeter and what that means for us with them being the perimeter, collaboration is the key to our cybersecurity readiness, resiliency, and success across all of these items.

Now, we're going to shift gears a little bit as well. When we think about ransomware specifically or cybersecurity in general, there's a few things that we certainly want to get right. There's certainly fundamental things, the blocking and tackling of cybersecurity, we have to get right. The tactics. The tactics, we execute. Tactics follow trends, so we certainly see certain trends occurring. We modify our practices, our policies, our procedures, and in our tactics to be resilient against cybersecurity, and again, it's all about people. All of this working together. We have to understand how we recognize people as a perimeter, mentioning that, letting them know that they're the perimeter. They're part of the blocking and tackling to win the day when it comes to cyber threats and then making sure that things that we're seeing, trends that we're seeing occur, what we're seeing from other agencies and partners, what we're reading in great publications, whether they come from GovExec elsewhere, how are we infusing that into the way in which we think about our work?

The way in which we can think about our work, especially for folks who don't think about cybersecurity or IT things on a regular basis, take them back to their home. Ask individuals, "In general, think about your home. What is the most connected device at your home?" And most everybody's immediately going to say, "Well, most connected devices got to be my phone," right? Absolutely. Sure, your phone is certainly a connected device. What else is connected at your home? Folks say, "Well, my TV. I've got a brand of a TV that is connected to my home," and it's like, yes, absolutely. That's a great example, and there's a whole host of other things too. My oven might be connected to my home, my toaster oven. I've got an Amazon Echo or I've got a similar type of device that's certainly connected to my home. I've got a smart coffee maker that helps me wake up in the morning.

I've got a thermostat that I can control from anywhere in the world, and it's connected obviously to my home. I've got monitors in my home. I might have baby monitors in my home. I might have other monitors in my home. I might have a picture frame, an electric digital picture frame that is connected to my home. There's lots of different devices. I've got sensors throughout my landscaping to understand the moisture level within the ground, and that gives me an understanding as to how often I need to water or what type of chemicals I might need or nutrients that I need to add. I might have certain other wall monitors in my home to see if an elderly person or a loved one has fallen or something of this nature. Lots of different things are connected. Smart plugs in our home that if we forget to turn off the stove or something. It'll switch off on its own.

These are all things that have helped increase our livability, increase our independence, increase our enjoyment, our efficiency. It's also increased the landscape of cyber threats. So, if you're not necessarily an IT person, we all benefit from IT, and we all understand that the threat landscape has increased over the years, and there's a number of Internet of Things activities that we are involved in within our work. Again, whether we're on the local government side or the federal government side or any aspect of that, we are working to build smarter water. We're working to build smarter homes within smarter cities, within smarter states, within smarter industrial areas and businesses and logistics and healthcare and everything that we're involved in is now becoming more and more connected.

The digital transformation of all of our work and lives is quite exciting. It's quite beneficial. It is also quite risky. It increases the level of risk that we have and further emphasizes this need for blocking and tackling and following the fundamentals of the work around cybersecurity. Some of the most common threats include things we've been talking about, phishing attacks that drop malware on our computers, ransomware, email attacks. In some cases, brute force and social media, increasingly so social media threats that we see and the whole AI movement that we're starting to see now because of natural

language processing and large language processing. Software and capabilities through AI are going to even further accelerate the threats of cybersecurity.

And not too long ago, our friends from CISA, MS-ISAC, Nas.io, NGA elsewhere came together and talked about what do we do? What can we do? And again, it's the blocking and tackling as to what they came up with. Back your system now and daily. Reinforce cyber awareness, training and education and update your instant response plans. It's the blocking and tackling of things. Part of the challenge of this is timing. It's like, "Do we have the time? Do we feel like we have the time to get into all of this, and do we have enough time to understand where are we today relative to these things? Where do we need to be in the future? And then how do we get there?" So, are we backing up our systems every day? You might know that for sure because maybe you're on the IT side.

You may not know, but it's a question to perhaps ask. Do we have the right training in place? What are we doing today? Can we be doing more? How do we know how much more? Where are we trying to get to? Do we have all the right instant response plans in place? Can we collaborate to move forward faster on getting those in place relative to where we want to be? The way in which we start with all this, and again, where we want to start is where are we, how do we get better or where do we need to be? And then how do we get there? Start with the conversation. If you're looking for a conversation starter, here you go. You can turn to each one of these. This is an assessment, an audit of any organization. You can turn each one of these into a question. So, maybe you're an elected official saying, "I don't really know where to start, but I certainly am really concerned about cybersecurity. What do I do?" And take this list of 10 things into your next IT meeting or your next steering committee meeting, your governance meeting, your next elected officials meeting to say, "These are some questions I'd like to ask."

Do we have full system inventory? Do we have backend recovery system? Do we have segmented network access? And for some of you might say, "I don't know why that would be important." It's like your IT person knows exactly why this is going to be important, and it starts the conversation. So, whether you are seasoned and experienced and educated in this area or not, you can certainly be... People are the perimeter. You can be the person bringing up these points of conversations. Do we have a trained workforce? Do we have password security? Do we have viewable file extensions? Do we have email server controls? So, we can turn each one of these into a question.

If you're on the IT side, this serves as your audit form, right? This is an assessment. You're going through it. Do we have all of this and you know that there are questions and some depth of context behind each one of these. The full system inventory, I mean, it's like, wow. First of all, we need to do that. We've got to get that. How do we understand that? Do we understand how many people have left in the last six months in the last year so that we can actually inventory their systems as well? Have they been turned back in? Do we have their key cards? Have we turned off their system access for physical systems as well as access to the cloud? All of these things, there's a context behind it, but it's a point of reference, and again, it starts the conversation. If we want to, we can turn this questionnaire, this assessment into an actual assessment on a Likert scale relative to best practice.

These tools are available. They're available through CISA. They're available through organizations like Cybersecurity Collaborative, as well as a whole host of others. If you're looking for places to start, you may even start with your insurance company. Do you have a cyber insurance? Do they have tools that they can provide? If you're looking for tools, use an assessment to learn, and if you want even more, this is 25 questions around determining your business continuity. Again, these are tools. We're not going to go through each one of these items, but we certainly wanted to provide to you some tools coming off the day of this event where you've really covered the landscape of threat vectors and threat actors and overall security risk that you're facing today and what's going to be coming up because of AI and others, but these assessments and slides here can be used just as points of communication.

The focus is on blocking and tackling. How are we defending, defending, defending the perimeter of our assets, including our people, our employees, and those that we serve every day? And these charts here can serve as reminders that it is all about people. We do have to focus on the fundamentals, and we do have to be mindful that we're going to be updating this on a regular basis because our tactics are going to follow the trends. This is simply a cheat sheet here as to things that you can do on a regular basis. Do you reboot your mobile phone every day? And it's like many of us don't, and sometimes I don't. I did do it today, but sometimes I don't, and it's like we should be rebooting it every day, so when we restart the computer, our phone or our laptop or other, when we restart the computer, it's doing a search to see what updates do I need to be making, and so are we doing this vigilantly?

Are we patching vigilantly? Are we using the most recent versions of the software that we're supposed to be using? If not, those are first places to start. Again, blocking and tackling and raising conversations, raising the question among people because people are the perimeter of what it is we're focused on, and collaboration is the key. We don't have to use GovExec materials and tools and charts. We can go to CISA. CISA has a wonderful assortment of assessments and tools, and if you've not been to CISA.gov lately, they've got great information on cyber essentials that you can see here on the screen and one of the things too that I want to bring up about CISA, they've got some of these checklists too for the IT professionals that are out there. If you've not been to CISA recently, please go and check out CISA.gov.

One thing too that I want to bring up relative to the center for internet security is they have what is referred to as the Nationwide Cybersecurity Review. It's free. It's free. It's available from October 1st to February 28th every year. Go in, you fill in information about your organization. There's no cost. It's completely anonymous, and it's a self-assessment. If your organization is not doing this, please do this. Please register your organization, your agency, your county government, your city government, your state government. Register for the NCSR between October 1, February 28th. Fill out the information.

Again, there's no cost. It's completely anonymous. You can learn information on your own here as you can see the website, and they'll give you a report. They'll let you know what you're not performing, what you're optimally performing well, and everything in between when it comes to your systems. Now, I will tell you, it does take a bit of time to go through. It is very comprehensive, so be sure that you or your IT folks are preparing for this and allocating some time to get it done because it will take you a bit of time to collect the information, present the information, provide the information, but it's free and you get information from... The Nationwide Cybersecurity Review will be a review specific for you and your agency.

So, if you've not done this, please consider doing it. If you haven't done it, there's a good chance your neighboring county, city, state has done this. Contact them. Ask them about it. If they are not familiar, contact us. We'll certainly put you in touch with the appropriate people or answer any additional questions that you might have. If you are affiliated with another organization, if you're a county and you work with the National Association of Counties, contact NACO. Contact the representative's NACO and ask them about this. If you're a city and you're part of the National League of Cities or you're a member of other agencies, please contact that association and learn more about this opportunity.

I want to just provide a quick thank you to each of you. I so appreciate the work that you do in the agencies that you work for, doing the great job that you do, protecting us from cyber attacks. Stay vigilant. Continue your great work, and if there's anything that we can do to help out, we certainly want to say yes at all possible opportunities that we have, and one thing, as I mentioned at the beginning, I do want to invite you to participate, free of charge, the GovExec Cyber Simulation. We provide this on a quarterly basis. We have predominantly counties and cities participating, but if you're interested, send me an email. Email me at first initial, last name, trahschulte@govexec.com for your scholarship. It's 100% free for the simulation.

If you also are interested in participating in our 12-week online fully facilitated Cybersecurity Leadership Academy, send me an email. We'll give you a scholarship for that as well. We can't possibly make that completely free of charge. There'll be a nominal charge for you. Our goal is to make leaders better, and we do that through the GovExec Professional Development Academies that we offer, the leadership programs through our simulations, and the leadership through our 12-week academies. They're here for you. Again, the simulation is free. The 12-week Cybersecurity Leadership Academy I think is like $2,000. If you would like more information about that, please let me know. Send me an email directly at trahschulte@govexec.com for your scholarship.

Again, thank you all for your participation in this GovExec event. If you haven't done so, look to the person next to you. Thank them for being here. Thank them for the great work that they're doing, and if you're tuned in virtually, pick up the phone. Call your neighboring county or your city or federal agency. Thank those individuals for doing great work for those that they serve, including us. We're all members in communities and cities and counties in which we live, and we're all trying to do the best we can to defend those organizations as well as collectively defend the country. Thank you all so much. My name's Tim Rahschulte. On behalf of GovExec, have a great day.