EDUCAUSE
Webinar | Connect It, Protect It in Remote Working and Learning Environments
Thursday, October 8, 2020
1:00PM- 2:00PM Eastern
Welcome to today’s Industry and Campus webinar -- Connect It, Protect It in Remote Working and Learning Environments. This is Jamie Farrell, Online Event Production Manager at EDUCAUSE and I’ll be your moderator for today. EDUCAUSE is pleased to welcome today’s speakers -- Peter Romness and Wendy Nather. I will introduce them in just a moment, but first let me give a brief orientation on our session’s learning environment. Our virtual room or learning space is subdivided into several windows. Our presenter’s slides are now showing in the presentation window, which is the largest on the screen. The tall window on the left serves as the public chat space for all of us. You can use the chat to make comments, share resources, or to pose questions to our presenters. We will hold Q&A until the end of the presentation, but we encourage you to type your questions into the chat throughout the Webinar. If you have any audio issues, click on the link in the lower left-hand corner. And, at any time you can direct a private message to Technical Help by clicking in the top-right corner of the Chat window. A drop-down menu will appear where you can select Start Chat With and Hosts. The session recording and slides will be archived later today on the EDUCAUSE website. And now, let’s turn to today’s presentation. We all have so many users and their devices that need to be connected, especially when working or learning from home, and we want to make sure they can connect easily while still maintaining the security we need. Zero Trust is a great way to approach this. It's based on the idea that trust must be earned before any connection is allowed, and that trust must be continuously monitored and verified. We want to make sure that users are who they say they are, not someone who stole their password, and that our devices are not corrupted. Zero Trust does not have to be hard. This session will help you understand what Zero Trust is and discuss how to use it to more effectively secure your environment and devices. We are delighted to be joined by Peter Romness. Peter is the Cybersecurity Principal in the US Public Sector CTO Office at Cisco Systems. For over 30 years, he has devoted his deep knowledge and diverse experience to help government and education organizations securely accomplish their goals. He works with NIST and the National Cybersecurity Center of Excellence and has contributed to their 1800-Series Special Publications. He is focused on helping leaders understand and implement the latest cyber strategies to defend against threats, maintain individuals’ privacy, protect sensitive information, and secure government intellectual property. Wendy Nather is Head of Advisory CISOs at Duo Security, now Cisco. Previously she was Research Director at the Retail ISAC, and Research Director of the Information Security Practice at independent analyst firm 451 Research. Nather led IT security for EMEA in the investment banking division of Swiss Bank Corporation (now UBS), and served as Chief Information Security Officer of the Texas Education Agency. Nather co-authored The Cloud Security Rules and was listed as one of SC Magazine’s 2014 Women in IT Security "Power Players, and an Influencer in the 2018 Reboot Leadership Awards. She also serves on the advisory board for Sightline Security. Thank you both for being here. And with that, let’s begin Today’s Industry and Campus webinar --
Connect It, Protect It in Remote Working and Learning Environments. Peter and Wendy, over to you.

>> Thank you.

>> Thank you. Today's topic is called connect it he, protect. Part of the reason is October is Cybersecurity awareness month and the theme is connect it, protect it. So I'm thrilled to have Wendy here with us today. She's one of our leaders and talking about Zero Trust and connecting and protecting and so Wendy, thank you for being here.

>> Yeah. Thanks for joining with me Peter. It's always a pleasure.

>> So the hot topic right now is remote working and learning and so it's very topical to talk about this. Today we're going to talk about this. We're going to talk about what's happening in the industry, what's making all of these changes. We're going to give you a bit of primer on what Zero Trust is. Then we're going to talk about how you can connect it and protect it. And then we're going to give you some resources. Let's get started with what we are seeing. Wendy and I were talking about and we said we're not going to (Indiscernible) of all of the facts that's going on. But there are some things that are important to point out. Do you want to comment on some of this?

>> Higher Ed has been an great laboratory for zero trust principles by the very nature. But now those of you who have joined us who are dealing with K through 12, you are stuck with students who are no longer subject to your web filters, on your campus network. You've got kids who are making very creative custom backgrounds. I've heard teachers plaining about that. And -- therein are a lot of students out there trying to get any kind of a connectivity. Otherwise they are stuck outside of a taco bell. Peter could -- do you want to go over that?

>> This Pandemic has kind of forced a lot of things happen that we're starting to happen. So all of a sudden, you know, where some people had trials of having people work from home or learn from home. Now, you have to. So not only was the technology changed, but the attitudes of people has changed. I think that kind of takes us to our next slide that we have. You know, in in the Cybersecurity business, which I've been doing a long time and Wendy has, too. We talk about attack mounted (Indiscernible) and from a Cybersecurity perspective. It's kind of -- we really increased our attack services and the number of holes that could be found.

>> Right. For one thing, in our athletic intelligence team, we have been seeing a huge rise just in the amount of Covid-themed fishing attacks and names being registered. The other problem is when everybody moved to long-distance, they had to do it in a hurry and maybe some groups that felt this is only going to be temporarily. They just put in whatever they could. And made it work and now it's looking like it's gonna be longer term. There's a lot of confusion are we going to be on campus? No. Wait. We're going to be off campus. People running back and forth and
that -- that confusion also makes it very difficult for everyone.

>> Yeah. And there's a big thing about throwing a lot of things at it quickly and now I think -- both for security and for connectivity. Now I think people are stepping back and saying this is going to last a little bit longer. What do I need to do to make this viable moving forward? So there's a little more intersection going on. And people are seeing this loss of control when things were on campus. We're seeing high -- you know, high-Ed used to have tons of the devices connected and now they have to connect those to their learning devices and there are more devices that they have to worry about.

>> Right. Around the assumption --

>> Go ahead.

>> Sorry. I was going to say the assumption was for administrative staff that they would stay on on campus, you know, and have access to everything that they needed. Of course, we also know that higher-Ed is not just about the academics. I think of -- my friend Helen Patton, she teaches at Ohio University. They are a hotel, hospital, veterinary hospital, they have a nuclear reactor. They have all sorts of things. It's not just the academic environment that's radically trying to --

>> Okay. There are a lot of things going on. That gets us to the next top take we would like to talk about. We're proposing as you make these things that you think about zero trust. Debt.

>> So with -- when we used to talk about connecting to a network, we had a boundary around the network, a perimeter, and users had to authenticate to the network, once they were in, they were given access to the resources of that network. That's kind of not how things are working today. Now it is -- the users can connecting to clouds for their data and for their applications. We have the users connecting from all over the world and -- and our devices, you know, it's not just user devices.

>> When you look at all of the decisions security-wise were being made, you know, with the data center at the center. You know, everything revolved around that and the assumptions that the users would be using standardized, standardized devices and now you flip that INSIDE out and you look AT the modern approach and -- where the user is at the center and planned and implemented. It is, what do they need? Where are they accessing things? Can we give them the same experience regardless of what they are using. What's really the heart of what Zero Trust is about.

>> That get us to this idea that there's no longer a perimeter and the -- now there is a new barometer which is any place that you make an access decision. And that can be anywhere. That's kinds of the basis for Zero Trust. And this gets to the idea of what we call a perimeter listing network. And so -- Wendy, do you want to add to this at all?
Yeah, that's right. There's always an argument about -- oh, the perimeter is dead. Is it not dead? It's not dead as to what we're actually thinking about what it means. And if you think of it about where you make an access control decision, that can be any layer. We're not telling you to throw out your firewalls but it could be at the application layer, the operating system layer and it might be all of the above, depending upon what you believe the risk is and where you can or must enforce those controls. See that's really the difference that, you glow, we're thinking in terms of a perimeter being a function rather than a technology.

Right. That brings us to Zero Trust. So this whole idea of having no parameter has been talked about in the industry for a long time. The -- in 2004, there was a group in Europe that got called, the Jericho group (Indiscernible). And they talked about this very issue. They came up with ideas of what it should be. And, you know, there wasn't a whole lot of action around that. And then a guy named John Kindervag came up with this term called Zero Trust. I gotta tell you, Wendy, I love voting you on this. I'm going to do this while you are here. Zero Trust took off because the other way to say it was too hard to say.

Too hard to say after a few years. I remember when this collaboration-Oriented architecture came out from the Jericho forum and I thought this makes sense. But I have no idea how I would be doing this. Now in the intervening team, we've involved technology a lot and have better tools for implementing the sorts of things that we always wanted to do and always that we should be dole. Let's take a look at what those might be.

I do want to say first, if we -- I think it is on the next slides, I do want to say first that I know a lot of people don't like the name Zero Trust, and it doesn't mean that we're not ever not trusting anything. That's impractical. What it means, though, is that we're not assuming any trust and we're thinking very carefully about what it would take in each case to earn that trust. What verification do we need to do and how often do we need to do? And what factors would that take? It's no longer, okay. You came in through the firewall, you are fine. What else do we need to know and decide with every access account? That's the many difference.

Yeah. And what I like to say is -- it's not about Zero Trust. It's not about least privilege. It's about earned trust and earned privilege for any asset that you want to get to in your environment. The idea of using all of the information you have to make a risk-based decision on who you allow to each asset. So that's the -- that's where I love to talk about it. There are three major areas where we've identified where I need to think about these risk-based decisions. And this is at the workforce, making sure that only the right users on the appropriately-secured device, get access to each application. This could be an application that's on premise. It could be in the cloud. It doesn't matter what application. But real important, each application. And then we talk about trusting workloads. So this is all of the apps and data in the different data centers. It might be a
include or on site and how do those apps talk to each other? How do they communicate? You need to make sure that these are protected and then these are all. Devices in your oh. They may be IOT. They could be network. You want to make sure that those are acting appropriately and before you give them access, you make them earn it.

>> Yeah, yeah. Exactly. You may be -- one of the principles described is continuous authentication. If you are making your human users a -- authenticate all of the time, they are going to be very crabby. Many may not realize the extent of the technology they have that's part of their university system that is actually internet connected and nobody is paying attention right now to weather those can be can you a authenticated before they connect to the network.

>> And I think that brings us to the next topic, how do you start looking at Zero Trust and your environment? And, you know, this is information that Wendy brought to this presentation and when I look at it, I see similar approaches and in many other programs. I work with the Federal Government and they have a called CDM and they talk about -- they first want to know what is on the program, what are the devices. They want to know then when is on the network and then they want to know what's going on in the network and they wanted to protect the network. And guess what? Is this very similar to that. Users and devices and applications, you know, what's -- what's -- yeah.

>> I want to encourage you who are listening, on the left-hand side in the chat or submit us your hardest questions. Type them in now as we're going along because I can imagine that if you see us talking about inventory of users or an inventory of devices, I can see you going, yeah. Right, like that's ever gonna happen. [Laughter]

>> Those things sound simple but we know they are very hard to do. The great thing with the technology that we're using these days, you have an opportunity to do almost real-time discovery. If you park a proxy in front of an application that everybody has to log into like E-mail. You will start to collect the information on who is connecting to it. What devices are they doing today?

>> One thing I've seen, there are often sometimes surprises about not only what is on the network but what's going on there. You know, Zero Trust is a really cool topic to talk about. And it's something that we're in encouraging you to look at. But often sometimes, it is engaging just good practice -- encouraging just good practice and good Cybersecurity.

>> And that's what we're struggling with the most. What cools can we bring to the table to start doing this incrementally.

>> And that brings us to the next slide, which is kind of where do we start? When I -- when we talk about moving forward, we need a plan in mind. No matter how you start, you need a plan in mind and hopefully this will give you some kind of direction on where to go.
I want to emphasize. Even though we're starting with -- you don't actually have. You can start when you can and make incremental improvements. It's just for a lot of organizations, you get the biggest risk reduction bang for your buck by implementing MFA. There's a blog post by Emery University that talks about when they first deployed MFA the number of account take overs, dropped over -- well over 90% and also the number of fishing domains that they had to block dropped by 90%. In a lot of ways not only does MFA work in across the board protection, it can be seen as a deterrent. They just stop trying. They take I out. That's why we took about that being a first step but, you know, if you think you can get farther by looking first to collect data on what devices you have and picking one policy, like can we just say that nobody should be logging in with broken devices? Can we just agree on that? Okay. Let's put that policy in and start implementing that and, you know, very slowly be the rising tide that lifts that. End be a Since dependencies then, this is very hard. This is something that you will start collecting data on and, again, you know, this is -- a multi-year journey. You might deploy an access proxy. As we mentioned, start grouping your authentication processes, so everybody has to hit the same proxy no matter where they are. One important story, a good story I heard from a CSO in the new buildings, they set them up like Starbucks. When you walk in there you get on the guest wi-fi. You got your coffee. You are working as if you are in a Starbucks. You don't get special access control just because you went in their office building, it will be the same controls no matter where you are. You can start thinking about that. Keep plying analytics and -- deploying Anna lettic, once you start to detect the anomalies, if you can't do anything about them, then are going to be a distraction. Peter what would say about the -- kind of the order of these things?

I love this order. The other thick I look at is how do you get a fast bang for the buck or a fast return on investment? Everyone laughs when you talk about return on investment for Cyber security. Looking for things that you can do -- that can gain you benefit with a little bit of effort. Go for a quick win. I see multi-factor authentication as one of those wins. It's very easy to set up. It's become easy enough for the users so they don't fight it. That's something that I always talk about as a good place to start.

Well, you know, we've seen a lot of college students who get very upset. It restricts their freedoms or something.

My daughter-in-law was in her M.B.A. program and was complaining about her -- I know, her multi-factor authentication, I said, you doesn't even have a little toggle thing that you have to type a number in. All you have to do is quick "okay." She said, oh, okay.

Yeah. I also want to emphasize that some organizations that start on the statistic journey, tended to start with the most critical applications or their most sensitive data. That can work sometimes but we found that other organizations have more success when they focus on a group of users who are the most forgiving and the easiest to work with and who look at -- and then THEY look at the applications that those users are using and start with those, even if they are not
the most critical. They are starting with the most forgiving population and working the bugs out of the process and then they expand to wider user groups and more applications.

>> So that moves us onto to -- I wanted to talk about some things that are critical for a mature Zero Trust environment. And, of course, the most important thing is trusted access which means that -- the whole idea of zero trust is that you are not allowing anyone access to an asset unless they are trusted. You have to go a good way of doing that. This involves not knowing who the user is but knowing how they are coming in so you can make a risk-based decision. What kind of device are they on? Is it the corporate or the government-owned device? That figures into your decision.

>> The ability to Microsegment -- excuse me?

>> [ inaudible ]

>> The ability to Microsegment is also critical. Think about it, you are trying to allow access only to appropriate resources. So, you know I want my students to be able to get to all of their learning. I want my teachers to get to their syllabuses and their benefits pages and I want my finance people to get to the finance resources but not anybody, you know getting to things that they aren't authorized for. So you have to be able to segment your organization one thing that really lays into that is threat intelligence. If there's a new threat in the world or if all of the sudden you find out that one of your devices or user has a new malware on their device, you need to be able to change your trust decision and revoke access or temporarily quarantine or temporarily just let them go to the internet and not anything else. So both this authentication, the granting of trust and the maintaining of trust so you can revoke -- if you need to it becomes important to automate that. How do you do that okay. Here we restructure typical remote users. This may be a student, staff, facilitator. You also have a school network, a school data center and you also have a cloud so your data and apps are in the cloud. They are -- what are some of the questions that you ask as you start to make these trust-based decisions. Wendy, do you want to take some of this?

>> Right. Around the great thing about Zero Trust is that, you know, again, we used to assume that there was kind of an authoritarian model in place. Somebody would make the policies and they would get pushed down. We know that that doesn't work very well with certain types of users in -- in an educational environment. They just won't sit still for it. What you can do is every time they are trying to connect, you can say -- you look at, first of all, do we trust the device either because we manage it or simply because we've seen it before. If you mark a device as belonging to a particular user, even if it is just there’s and even if you want manage it, but you say, okay. This is Wendy's phone. We've seen it before. We know we are going to see it again. That's already shrinking your attack service. So if somebody steals my credentials and they -- they steal my second factor, they would also have to steal my access device in order to get access. You can silently steal user's credentials, but if hardware goes missing, somebody steals
my phone and my laptop, people are going to notice. Another question you might want to --
ookay. We don't know much about this device but is it configured securely, you know, according
to the standards. Does it have a lock screen? Is it using inscription so you can kind of guess that
this is probably safer even if you haven't been managing it. Another question, is it currently
compromised? You look at whether it is configured and whether somebody has been brushing
their teeth regularly but you don't know if they have cavities. Well, we can see if they have
cavities right now. We will can say, look we don't care if you are looking at public pages with
this dirty device, but you can't log into the HR system with this. You can do it on your own time,
but you are not getting access until this happened. So let me give you an example of how this
would work and how it actually works quite a lit, is that when a new version of software comes
out, especially to patch a particular vulnerability that we know is being exploited. You may want
to say to your users, you know, you've got two weeks to update to the next version of the
software before we start letting you in. Now, again, you can do whatever you want with your
device. You are going to have to be up to date in two weeks' time. If it's a really urgent problem,
you can shrink the grace period. In fact we do that, around we say, you know, usually you have
two weeks. This is very serious exploit. It's in the wild. You have three days. If you don't update
in three days, you are not getting access. You can block access for everybody until they update.
There are a lot of different ways that you can use the answers to the questions to decide how
much access you are going to give and when. Some of the things that you want to do is protect
your users and so -- just an example that I use is DNS protection and that's what the third bullet
down on the left says, are the devices connecting to unsafe entities. You want to be able to
protect your users being infected in the first place, and if they are taking them to wad websites,
these a good way to get infected and mess up our Zero Trust environment. We want to make sure
there is not happening. There are a lot of things that you -- you know, they aren't tied to Zero
Trust and -- until you start talking about this threat -- threat 9/11. You know, knowing what
threats are out there. But then they become very important. Okay. That brings us to some
principles that Wendy and I were talking about, that we really think people should think about
when they were going for Zero Trust. So the first one is, you know, it doesn't matter what you
call it. You probably already have been doing a lot of Zero Trusts and really, a lot of is good
Cybersecurity practices and everyone was moving towards this stuff anyway. But Zero Trust
gives you a nice way of looking at it. It's a way of thinking.

>> Yes, that's right. And then also, again, think about different ways of implementing these
principles -- schedule is not a -- Zero Trust is not a given technology. If you can question your
assumptions and start thinking about how you can implement this not just for your users but for
anything that you can connected to the network that you are responsible for as well as the
applications that you are using in your ecosystem regardless of where they are.

>> Right. Don't just think people. Think about who can get to it. Think about your apps and data
and think about the devices in the organization. make sure to apply Zero Trust principles to all of
them. And then Wendy and I were both in agreement on the next one, making implemental
improvements. Zero Trust is a journey. It's not a destination that you will get to it quickly. Many
people say you never get to it. A person who works with Wendy calls it a lifestyle choice. It really can be. I will attribute that to Sean Frazier of DUO. It really is. It's a way of looking at things, it's a way of making the appropriate decision.

>> That's right. You do want to think long-term and you want to be creative -- for example, I'm not recommending that you do to. So Peter don't listen, but if you implemented MFA for everybody and the only thing that you did was you registered everybody for MFA and you registered your device, you would still be shrinking THE attack service because whenever any -- they wouldn't have to use MFA unless they switched to a different device. You are protecting against somebody who steals those credentials. Any system using the credentials from a different device that's not remembered, then they would hit the MFA. That's really quick and dirty. I wouldn't necessarily --

>> That's --

>> But it is a large improvement if you are thinking incrementally instead of oh, my gosh we're doing a huge digital transformation. This is the kind of thing that you can think about starting with and then building on top of that afterwards? Also we know that institutes of higher elevation are struggling right now. You know, you don't know what your budgets are only going to be. A lot are trying to hold onto what they have. Questions that you can ask yourself are, if you are -- if we're just using how we are right now, how can we use it better, how can we add additional factors or change our processes so we're verifying more things. So that's another way to think about it. If you are doing geo location, that's fine. Just don't let it, the only thing that you are granting access on because that's what Zero Trust is kind of a reaction against, is that -- that I.P. address used to mean location for us. We know it doesn't work. It can be spoofed. You can still use it with enforcement, but it is better to add other things like checking the state of the.

>> If you have an unlimited budget, you -- and most people don't, you have to make the best of what you have. But just making those decisions goes a long way in making your environment more secure.

>> You don't have to say the word "Zero Trust" to your manager. You can refer to Google's beyond (Indiscernible). You can call it entity and edge security, which is what chase Cunningham at Forrester who is their principal analyst. That's what he calls it in his book. He CALLS it entity and edge security. Think about it. Maybe some way -- Peter, you know the joke about what do you call alternative medicine that's been proven to work? Maybe we'll just do it -- call it security. You are probably doing it already and the question is where do you go from here and where can you start making more changes?

>> Yes.

>> Do you have any other tips for folks Wednesday.
There's a -- what about password less? I know some people are very interested in that topic. And password less to my mind is part of the process of smoothing our users' access experience. I owls thought it was a stupid idea to store this in organic material. The other big mistake that we as professionals made is to tell the users never to write their passwords down. So we kind of created the problem that we have, we're trying to point out that -- I want to point out that -- this is the five-day forecast way that you can start using the passwords. It's not that we're going to throw passwords out the window, but we'll reduce the amount of time that users have to rely on them. And that's another thing that people are exploring today. If you are using single sign on and you are simply extending THE length of session time for log-ins for applications. You are reducing how often your users have to use their passwords. If you start MFA or you start to add these other factors that are increasing and then you can think, did we need this password? Those are very early days. Some of the ways that we are implementing password less thanks to new standards like web authenticator. We have enclaves in mobile phones computing models in laptops means that we can use cryptics that cannot be directly accessed by the user, instead of using passwords. If I could just authenticate this, I would be a really happy camper. This is what we're kind (Indiscernible) for I know that you are working in wild, wild west environments and this may sound like a pipe dream to you. Certainly, this is not going to happen tomorrow that will be implemented tomorrow, but again, as long as we're exploring possibilities with Zero Trust, what factors can we use, what policies can be implemented? We are starting to touch on what is possible. I would encouraging you to keep thinking and talking with your peers. Even if you are not going to be able to jump into this today, how can you start aiming towards the future?

And just kind of --

Kind of -- kind of an example of the Zero Trust thinking, when you start to think about passwords. When I think about it in a Zero Trust format, I think about it as another decision on whether I'm going to allow access to a particular asset. You may log in and be able to log in with your face or your thumbprint or by your device to get to more things that the security isn't as important. And then if you want to get to financial data or personnel data, you have to do something else to build the trust that you have in order to get into the asset. When you start applying Zero Trust thinking, that's a good example of how it goes and the whole name and password becomes another factor.

Yes. That's right.

I was just thinking of one of the questions that we hear -- what are organizations' biggest struggles when they are trying to implement zero tut? Go they start saying Zero Trust and we want to do the project, the first thing their management asks is how long is it going to take. How much is it going to cost.
It's very hard to know because, again, this is not one box that you are going to put in. It's not one technology. It's not even one project. It is -- a lifestyle change. A bunch of different ones, I would advise organizations not to treat it as one big project because that scares management but to start thinking about doing everything going forward in a trustee way. So whatever project, you are taking on, whatever you are going to add, fine. We're going to do this in a Zero Trust way. Another big problem struggle they run across, these sorts of controls are crossing functions. They are going against desktops, other equipment, mobile. A lot of different organizations have different silos for these organizations or as I like to call them, cylinders of excellence and getting this activity and the policies to cross all of the silos and bridge them, I don't know. We can't do that part. That's the mobile team's job do could. This is another thing that you can start working on now organizationally working horizontally and thinking horizontally.

Where's going to move onto our last thing, which is resources to help you. But in the meantime, if you would think about typing any questions that you have, then Wendy and I can address those once we've gone through the resources. So one thing that Cisco does, most of this is available on a trial basis. If you would like to try the really any of the Cisco products. Contact us. If you know who your sales rep is, ask them, otherwise you can contact me and my E-mail address is on the next slide. And then we've also given some links that you can connect to get more information. We have a really nice one-pager on securing remote learning. Cisco has an all in one security platform that's free called secure-X that allows you to see the security devices together so you can see and respond to threats bigger. There's more information on that. We have we have a whole education organization that does things with web X and collaboration as well as security and networking. That's helpful and then we have some pretrials and a video explainer. My contact information is often the bottom right, with that --

Yeah and I want to point out if you are not familiar with Adobe connect, these links are live. These links are hot. If you want to go open those right now and leave those tabs for, looking at later you can crick right now.

It doesn't document like we don't have any questions yet. I'm going to close out by saying thank you very much for joining us. I hope we answered a lot of questions. Hopefully, we gave you some food for thought and if you need any help or question, please contact us. So thank you.

Good luck to everybody. If you have any questions, feel free to right them in the chat. You can reach out to Peter. His E-mail is in the slides and aa copy of the slides will be posted on the website later.

Before you sign off, please click on the session evaluation link, which you will find in the chat window. Your comments are very important to us. Again, the recording and the slides will be posted to the website later today. Please feel free to share it with your colleagues and join us for the next Webinar at October 13th. At 1:00 eastern. On behalf of Du, this is -- of Educause. This is Jamie Farrell and thank you for joining us today.
End of Webinar