Cheryl Dowd, Senior Director, Policy Innovations, (00:00:00):

Give us to the first slide, please.

Cheryl Dowd, Senior Director, Policy Innovations, (00:00:09):

Well, welcome, everyone. This is part two of the cybersecurity webinar series that's being brought to you by the State Authorization Network and WCET. We're very pleased that you could join us today. Part two of this cybersecurity webinar series is in regard to the postsecondary cyber risks that are associated with third parties due to ransomware. Could we go to the next slide, please?

Cheryl Dowd, Senior Director, Policy Innovations, (00:00:33):

I'm Cheryl Dowd. I'm your host. I will be turning this over to our moderator in just a minute, but I just wanted to welcome you and tell you a little bit about SAN and WCET. Could we go to the next slide, please?

Cheryl Dowd, Senior Director, Policy Innovations, (00:00:46):

WCET developed SAN, so I'm going to talk about them first. WCET is the WICHE Cooperative for Educational Technologies. They are a membership organization that has been serving institutions and organizations for more than 30 years by addressing practice, policy, and advocacy for the development of quality digital learning and higher education. And as I was saying, WCET developed the State Authorization Network, which is also a membership organization of more than 800 institutions and organizations nationwide, for which we serve the members to empower them to successfully resolve state and federal regulatory compliance challenges to improve student protections in digital learning across state lines. We can move to the next slide, please.

Cheryl Dowd, Senior Director, Policy Innovations, (00:01:31):

So, today we have a very robust webinar for you. It's full of content. And because of that, we do want to take your questions, but we will be primarily taking the questions at the end of this presentation. So we would appreciate if you would use the Q&A. Actually, this says the chat box, but could I ask you please to put your questions in the Q&A box because that will help us preserve them. And if we are not able to get to all of the questions today, we will be able to talk with our presenters about getting answers to your questions. So if you could please put your questions into the Q&A, that would be very helpful. Could we go to the next slide, please?

Cheryl Dowd, Senior Director, Policy Innovations, (00:02:16):

Right now, I'd like to introduce you to a member of the SAN team. Kathryn Kerensky is the director for Digital Learning Policy & Compliance, and she will be taking us through the webinar today. So Kathryn, I'm going to turn it over to you.

Kathryn Kerensky, Director, Digital Learning, (00:02:28):

All right. Thank you, Cheryl. I'm really happy to be the moderator for today's webinar. Hope everyone's having a good day so far. If we go to the next slide, I'll give an overview of today's content. Today's presentation will consist of an overview of today's risk landscape and real examples of ransomware and ransomware attacks, along with third-party management and strategies to protect the institution. At the end of the presentation, we'll have some time for questions, so please use the Q&A box for questions.

Kathryn Kerensky, Director, Digital Learning, (00:02:59):

On the next slide, if you go to the next slide, please, I'd like to introduce our presenters. We're very happy to have David Sonheim and Tanya Taplin. Dave currently serves as the chief of Cybersecurity at the Cybersecurity and Infrastructure Security Agency, or CISA Region 8. Tanya is also with CISA Region 8 and is the state cybersecurity coordinator for North Dakota. We're so happy to have them both with us today. And with that, if we can move to the next slide, I'll pass it over to Dave and Tanya to begin their presentation. Thank you both.

David Sonheim, Chief of Cybersecurity (00:03:30):

Okay, Kathryn, thank you so much. Yes, Tanya and I are here to try to cover some content for you. Again, it's really all about trying to share information, gain awareness as we cover the material. So, happy to hit any questions you have. Go ahead and put those in the question and answer, as Cheryl stated, and then we can kind of get right into it. Kathryn, just so you're aware, I'm not currently seeing the slides, but I believe you that the slides are up and going. So I think we can move to slide number two.

David Sonheim, Chief of Cybersecurity (00:04:03):

And I assume we're on slide two. Okay. So as introduced, if you didn't attend the webinar number one, we are with the Department of Homeland Security. We are with a separate agency from the Department of Homeland Security called the Cybersecurity and Infrastructure Security Agency. You may not heard of it. Think about it as its own separate agency that kind of has three areas of strategic goals. The first one is the lead agencies for the defense of federal civilian, .gov, environment and networks. So think of those executive federal agencies, kind of a compliance mission as well as a securing them. And it's really more than just cyber, it's really both physical and cybersecurity. But the idea is to be that central organization, central agency, to take care of the federal executive agencies.

David Sonheim, Chief of Cybersecurity (00:05:03):

The second part, the mission kind of expands and goes a little further than that. To some areas, we talk about national critical functions. So, those functions that help us, United States, conduct and perform everything that you think from a lifeline. So that could be healthcare, that can be water sector, that can be state and local government. And really, the idea is to do the outreach and the preparedness efforts for both a cyber and a physical threat. The next piece is to really do an outreach campaign, which is part of what we're doing here, at no cost. That includes assessments, that includes webinars, any promotional piece that is part of that preparedness. And that's really both on the physical and cybersecurity, connecting folks with the resources, tools, assessments, et cetera, to try to help bolster their preparedness. We can move to the next slide.

David Sonheim, Chief of Cybersecurity (00:05:55):

Okay. So for today, obviously, Tanya and I are going to break it up. I'm going to do the first part and hit some of the fundamental pieces, what we've seen in the past, both from a third-party risk perspective as well as the ransomware or cyber threat activity. We know that both the learning management system vendors as well as the online program management companies, that I know all of you work with and interact with every day, and I know that all of you heavily depend on those to deliver the digital learning by leveraging that technology and platforms as higher educational professionals. And so we're going to try to make it very specific in that realm for you to try to connect it with everything you work on every day. We know that higher education in general, from previous incidents, whether that be a ransomware attack, a data breach, null service, unfortunately aims at higher education.

David Sonheim, Chief of Cybersecurity (00:06:52):

We know that the community in general is a very trusting community. We know that we like to promote the sharing of knowledge and information sharing. Unfortunately, that kind of contradicts what cyber adversaries like to go after. And so that's unfortunate, but they definitely see the higher education sector as kind of a soft target. They know that they're probably not as much rigor. We know that it's more of an open environment. So that's part of the reason, and Tanya will hit it later in her slides, of why unfortunately higher education becomes kind of a target. Now we can move to slide four.

David Sonheim, Chief of Cybersecurity (00:07:27):

So we talked about this term a lot. Over the last two to three years, we have definitely seen this risk of ransomware absolutely exploited. We know that cyber threat adversary, once it gets presence, it knows that if it can lock up the organization's data or infrastructure or systems, unfortunately that gives them a leverage point to try to extract some type of a payment or some type of ransom. We know a lot of those unfortunately go unreported. Although we've got some data around it, we know there's also a large or higher volume that unfortunately are not being reported, meaning the statistics are much higher.

David Sonheim, Chief of Cybersecurity (00:08:11):

We know that these types of effects or these type of attacks are extremely disruptive to your environments. We know they have a significant impact. That's really why we're trying to foot stomp this entire issue or concern connected also to the learning management programs that you support every day, which kind of starts us to get into the third-party risk piece. And we know that, unfortunately, a lot of those vendors, we can't directly influence them. But the idea there is to give you some key examples of what we see in the past, where even though the university had good procedures in place, unfortunately some of those third parties create an undue risk, which resulted the event.

David Sonheim, Chief of Cybersecurity (00:08:56):

So, that's really what we want to do today, is to try to share information around that. We know that we kind of call that, or the family of that is what we kind of call supply chains. And that can either be a direct software supply chain, or that can be a vendor or a distributor or someone along that line that is providing a critical service, or maybe you only get it from one vendor, and if that vendor's not available, then you can't get the service. And so that's what we're trying to hit today. And we can move to slide five.

David Sonheim, Chief of Cybersecurity (00:09:29):

So I kind of promise just some statistics here. I don't know the statistics themselves are the driving factor, other than to tell us that we know it is on the rise. And we know that the amount of money that is demanded in the ransom is not typically what's paid in the ransom, meaning that there's actually folks whose job and role in the world is to negotiate with these threat actors to try to come to that dollar amount. I think that the takeaway here is, unfortunately, from a risk perspective, and we talk about the folks in risk management, we don't want their perception to be... Well, we can just pay the ransom. We have seen through various cyber incidents that a strategy of thinking that we'll just have more cyber insurance and pay the money, that has not worked out very well.

David Sonheim, Chief of Cybersecurity (00:10:22):

A majority of time, you do not get all of your data back. The data that you do get back still could have problems. The de-encryption piece that they actually give you when you pay the ransom can take an enormous amount of time to de-encrypt. So, all we're trying to say here is, if we can spend time in some other areas on the preparedness side, we really try to avoid the issue all together. We know that at some point in time, more than likely there will be a breach, but the more work we do to create redundancy, we don't all of a sudden put ourself in a position where we are forced then to do nothing but to pay the ransom. And that's really, at the end of the day, what we're trying to get after here.

David Sonheim, Chief of Cybersecurity (00:11:01):

Higher education institutions, as we talked about, can be a little bit difficult to defend and protect. We know that the vast and robust amount of information technology that surrounds the entire work we do every day, paired with some of those third-party learning management systems and online program management solutions, just make it very difficult. How do I protect it all right? And so the risk landscape is enormous. There doesn't ever seem to be an edge that we can defend backwards from. It seems to be across it. And so that's what we're trying to help get the point across here, is that we've got to integrate those kind of protections or those kind of controls along all of it and try to hopefully put some obstacles in the cyber threat actor's way, meaning that if I can delay, if I can prevent them from moving down their kill chain by putting controls in place, by putting two-factor login in place, by putting other activities like that, then I am hopefully putting the cost too high in the threat actor and it'll move on to somebody else who's not doing those things.

David Sonheim, Chief of Cybersecurity (00:12:09):

Unfortunately, we don't want to see somebody else get attacked, but at the end of the day, what we're trying to say is, as many of those kinds of controls just help you improve your overall resilience to these kinds of things. We also know that it's tough to get enough IT people or enough people that are focused in this area to try to help defend it. So we also know that that becomes a constraint and a difficulty as well. We can move to on slide six.

David Sonheim, Chief of Cybersecurity (00:12:40):

We did some analysis over 2021 where CISA did a special project with a group of higher education organizations and tried to look at what is the consistencies we see. Some of the terminology on the slides, let me see if I can help break that down for you. What happens is, whether it's Microsoft or another vendor, periodically, they will identify a vulnerability that needs to be created. And what we call these are known exploited vulnerabilities or KEVs. So these are exploits or vulnerabilities that are being seen in the wild. And the idea is, the more awareness that people have with these vulnerabilities, the better they can start to patch or remediate ahead of time. And so in this findings that we had, basically what they said is, out of 244 educational entities, we know that a preponderance of them had these known vulnerabilities still outstanding, meaning that there was a patch, but for whatever reason, it wasn't applied, leaving them in a upside out risk perspective. And so that's kind of what the data showed us there.

David Sonheim, Chief of Cybersecurity (00:13:46):

We know that in this one, they had 33, but older operating systems. Right? The reason we moved the next generation operating systems is, we've already applied all the fixes and the patches and made it hardened. But unfortunately, when you leave those legacy systems up and operating, you're just giving yourself another attack service for the actors. Okay. And then I think the third one there is, we know that people have done some work to decrease their exposure to these vulnerabilities. And I think the statins in there, 16.7%.

David Sonheim, Chief of Cybersecurity (00:14:16):

So the idea is gain awareness of vulnerabilities instead of being reactive to and develop a proactive approach and try to patch and remediate as quickly as you can. Those legacy systems or the pieces that kind of fall within the cracks there put some other controls in place. Because you know if you leave those vulnerabilities there, unfortunately the threat actors, you're just making it a little too easy. Think about it as an easily unlock door that absolutely should have been locked.

David Sonheim, Chief of Cybersecurity (00:14:41):

And we know that there's also some risky services in there, so the last bullet there is really talking about some of those services that we use to maybe do remote work, maybe have folks come in that are part of maybe our science or engineering department or our research department. We're not forcing them into the same amount of controls that we force other people, being that all of a sudden, we've got these risky things going on. And even though we're doing this good work over here, we're still leaving this easy door for them to come through. Now we can move to slide seven.

David Sonheim, Chief of Cybersecurity (00:15:11):

Okay, so for this webinar, I could not find a better example of an incident that happened regarding a third-party vendor that actually led to a ransomware of significant event for a university. So CU Boulder unfortunately experienced this event. This Accellion solution is basically a file transfer appliance. So as part of their work of the university, obviously I'm sure most of you have seen this as well, there is a requirement to move large amounts of data around. Sometime, that data is very sensitive, et cetera. And in this case, they were leveraging this solution made by this vendor to do this activity. Because this was living on their network when this vendor had a significant vulnerability, CU Boulder, even though they were doing great work to protect the university, all of a sudden now had an exposure due to this vendor. And.

David Sonheim, Chief of Cybersecurity (00:16:09):

So, in one side of the coin, you could say we want to point the finger at the vendor, but the reality is, now in this case, the vendor became a victim too. Right? The vendor didn't purposely do this. The vendor is also just like everyone else trying to work and trying to produce the best software they can. But in this case, this vulnerability caused a significant event for CU Boulder as well as multiple organizations as well. This third-party risk, we don't just see this in the university space or this software; we see it across multiple organizations.

David Sonheim, Chief of Cybersecurity (00:16:42):

The idea is, when we incorporate and embed these software solutions into our own environment, is to find some way to create a balance in that, that we don't automatically inherit that risk. Right? The idea is, understand what is in there, or what we call software bill of materials. What are all the components that are part of that software? How does all that interface with our systems? And try to create maybe some standoff distance so that when they have a vulnerability, we have an ability to isolate and not automatically inherit that. And so that's really what happened in this one. Unfortunately, the initial threat actor with the Accellion vulnerability allowed this ransomware group. Their tag name, their lingo name, or whatever you want to say, is CLOP. They were, during this time period, was a pretty significant threat actor that was going out there and doing ransomware.

David Sonheim, Chief of Cybersecurity (00:17:33):

So 300,000 records, the private, sensitive information, they didn't talk about healthcare information in this one, but definitely PII-related information. The threat actor tried to get 10 million out of CU. CU never disclosed the exact amount with this one. And I don't believe CU ever negotiated to pay this one. They were able to recover for some backup, but the idea is, that personal information was absolutely lost. So to say that, did the university lose uptime? Did the university not able to deliver content? I'm sure it was disrupted. In this case, the bigger issue was, all of these records got compromised, and now you're going to have to pay for identity protection for all of these individuals because it was so embedded in the environment.

David Sonheim, Chief of Cybersecurity (00:18:25):

So my guess is, the lesson learned when it comes to third-party breach is, the damage can continue to exist within the organization for a very long period of time. And the side effect then is having to pay for that identity monitoring service for an extensive period of time because you are the owner of the data when this event touched to happen. So, unfortunately, this was a prime example of when this went down. The impact to the university, I know they worked long and hard to recover from this one, but this is a prime example of where some of those third parties can become an upside down risk. And I think we can move to the next slide. I think it's slide eight.

David Sonheim, Chief of Cybersecurity (00:19:07):

Okay. This one, and I mentioned the Accellion, they actually had another vulnerability that hit last week. There was a lot of activity and news about this last week in the cybersecurity community because they know they're, what we call, a zero day. And so for those of you who aren't familiar, when we find a hole in a piece of software or some people's software that can be manipulated by an actor, before there's a patch, we kind of go in this window where there's no patch, there's no way to protect us. That little timeframe, we happen to call a zero day. So on the cybersecurity side, we obviously encourage people, if we know there's availability and we know there's a patch, get the patch done.

David Sonheim, Chief of Cybersecurity (00:19:52):

In this case, getting ahead of that zero day or getting visibility on what we call that zero day is absolutely critical. And so as soon as we start to hear about it, or possibly a proof of concept is developed by a threat actor, it gets a lot of attention. And unfortunately, this one, part of this Accellion software suite actually had a zero day that hit last week. And so lots of institutions as well as corporate America that uses the software was under a pretty tight timeline to get that corrected or to get some mitigation in place. The vendor actually provided some specific guidance to put some controls in place while they could work on a patch.

David Sonheim, Chief of Cybersecurity (00:20:30):

If you want to learn more about the zero-day market, there's actually a book done by Nicole Perlroth. The title of the book is called This Is How They Tell Me The World Ends. And she gets into the entire zero-day marketplace and how exploits are sold and all of those things. So kind of like a investigative novel there, but it's a really well done book that helps understand the problem in general with zero days. I think we can move to the next one.

David Sonheim, Chief of Cybersecurity (00:21:02):

Okay. This is an example right here, local to us, Regis University. The reason this one is an important case study for us to look at is, this threat actor more than likely had presence in this environment, but they did not do their activities when they had their initial presence. They waited till the most critical point, which is obviously in August, September when school was starting to get started. And that is when they decided to really infect their madness, lock up files, and really impact Regis University during a very critical time when they're trying to get their entire university up and running, and trying to get students registered and enrolled and get classes going.

David Sonheim, Chief of Cybersecurity (00:21:46):

So, all I would say from the takeaway on this one is, this ransomware threat is serious business. These threat actors are raking a significant amount of money. It's not a couple kids in a basement. It is a well-organized criminal group. They form corporations, the subsidiaries. They have folks that go and get this access. So they will strategically decide when the best time is to extract a payment. And in this case, unfortunately for Regis, it was during this critical time period. Now we can move to slide 10.

David Sonheim, Chief of Cybersecurity (00:22:18):

Okay. So on the DHS side, one of the things we do to try to assist organizations with getting their hands around, how do I manage all these vendors? What is a method and a process that I can use to try to improve my third party or my external dependency, my risk along that? And so this is a model that Carnegie developed, Carnegie Mellon University, their science and engineering department. And when we go out and do assessments, I could come out and do an assessment and try to assess your third-party management, your dependency program. And if we were to do that assessment, you can see that we would focus on how is the relationship formed, how good of a job are we doing on the management and governance of our vendor management, and then what are the protection and sustained requirements that we implement because of the criticality of what we do.

David Sonheim, Chief of Cybersecurity (00:23:08):

When we do the assessment, we kind of go around those four areas that you kind of see in the middle. What is the process and procedure for establishing and maintaining this plan? If we're going to do this activity, we should have a plan to do the activity. If we establish these relationships, we should have a process and a means and a way to quantify them through service-level agreements about exactly what's the details and that relationship. Once we establish that, then we need to manage it. What does manage mean? Manage means we have criteria that they need to meet in order for us to continue our partnership. And if they fail to deliver or fail to apply patches or expose us to a certain amount of risks, then at some point in time, we have to be done with that one and move on to a different vendor.

David Sonheim, Chief of Cybersecurity (00:23:53):

The last part of that obviously is, part of the way that we get an assessment of our top tier vendors for our low tier is, we monitor how well they perform over a period of time and we start to categorize or class them. That way, we are only doing business with that top tier in theory, to try to reduce our risk as well. So if any folks are interested in that, both Tanya and I go out as well as the other cyber advisors in the region, and we do these kinds of assessments. And the reality is, until you go through one of these assessments, you think your program is performing okay, but then you actually look at the details or combine it towards this model or this methodology as a rubric to go forth and say, "Wow, we really do have some work to do in this area. This helped us focus in on some strong areas and maybe some gap areas that we can try to improve our process." And I think you can go on to the next one.

David Sonheim, Chief of Cybersecurity (00:24:44):

So as part of this and their survey that they did, they went out and did a check with organizations, and not just higher education sector but across multiple sectors, to truly understand, are people implementing service-level agreements that are holding certain vendors? Especially vendors that we are ultimately dependent upon their software solution, their learning management solution, et cetera. And if it's compromised, we're compromised. Are organizations adapting their contract vendor management and that third-party risk to actually include some cybersecurity dependencies? So that way, we really understand before I do the work to contract with a vendor. I've got a better idea, from a risk perspective, what does this look like and how much risk am I associating? And what do I need to specifically include in that service-level agreement around cybersecurity, around privacy, around data protection?

David Sonheim, Chief of Cybersecurity (00:25:39):

So you can see here in each one of these, unfortunately, when they asked the questions, there was a no across the board, meaning that folks are still working to adapt to this thread environment and include this kind of rigor into these agreements so that we have some kind of a level playing field with the vendors where they don't assume any risk, and we assume all the risk. Right? So the idea here is to try to bring the entire population up, include these activities, and ensure that we have a program ahead of the time to try to manage and get ahead.

David Sonheim, Chief of Cybersecurity (00:26:09):

So hopefully, that kind of gave you a start to the presentation. But at this time, I think we're on slide 12, and I think I'm going to kick it over to Tanya. She's going to pick up from here and talk specifically about higher education type risks.

Tanya Taplin, State Cybersecurity (00:26:22):

All right. Thank you, Dave. Like Dave, said for the next part of the webinar, we're going to go ahead and we're going to talk about LMS and those other third-party vendors, and some of the privacy issues we need to be concerned with, and what we need to do to help make higher educational institutions be more secure. You can go ahead and hit the next slide.

Tanya Taplin, State Cybersecurity (00:26:42):

All right. So here we've divided the third parties into LMS providers and online program management companies, which most of you are probably going to be familiar with already. I personally have had experience with about half of these on the list, either as a professor, as a student, or as even a parent. So LMS and OPM apps, they are popular targets for attackers because hackers know that gaining access to these apps is easier than penetrating your school's defenses. They also know that they only once have to get access into the app, and then they can use that as a foothold to spread their attack. If hackers find a vulnerability and are able to exploit it at one organization, then it's likely that they will be able to take that vulnerability and exploit it with other organizations. So if this involves ransom, at the end of the day, this can end up being a really big payday for them. Next slide.

Tanya Taplin, State Cybersecurity (00:27:47):

So what are these known vulnerabilities? Vulnerabilities exist. We know that. It's vital that whomever you designate to administer your LMS system, that updates are installed and that the system is monitored for those vulnerabilities. Include yourself in those notification lists from your vendor. Half of the battle sometimes is just having the awareness of those vulnerabilities. Sometimes when we think of hackers, we think that they're actively trying to just let break into our systems and that's how they find those vulnerabilities, but it's much easier than that. Attackers don't need to work very hard to find those vulnerabilities.

Tanya Taplin, State Cybersecurity (00:28:28):

For example, this past weekend in a pen testing class that I'm taking, part of my assignment was to pick a target and to gather information. And naturally, because of my previous work history, I picked a college campus in the US. I Googled them. I went to their website, and one of the first things that I saw was a link to their LMS, which is actually exactly what I would expect to see. Students need to be able to get in to see their assignments, to submit them. So what did I do? I went out. I did a simple internet search on vulnerabilities to see what kind of vulnerabilities that I could find. So what did I find? There was the common CVE list, that common vulnerabilities and exposures. Website that Dave had talked about earlier, it had hundreds of known vulnerabilities. And there was one, within the last couple years, scoring a 10. And if you see a 10, that's going to be the most critical.

Tanya Taplin, State Cybersecurity (00:29:27):

This vulnerability, when exploded or exploited, allowed an attacker the ability for remote access. So some of the most common vulnerabilities you will see allow attackers to gain remote access. Once they do it, it's really only a matter of time before they're going to go ahead and elevate those privileges to that of a teacher or an admin. So if elevating to a teacher, they can retrieve test scores. They can modify grade books. And if they're students, they can be their own grades, they can be other grades.

Tanya Taplin, State Cybersecurity (00:30:02):

I've actually had a previous student, although this didn't happen in one of my classes, but it was a student, he wrote a script. And when he ran it, it allowed him to retake a test that he had previously taken and it automatically populated the correct answers for him. So that's just one example. SQL injection, those are vulnerabilities that can allow malicious actors to create secret admin accounts for use later in malicious code. And that could be not necessarily this week or next week, that can be when school starts like we saw earlier, that Dave mentioned in his example. It can be six months down the road. Next slide please.

Tanya Taplin, State Cybersecurity (00:30:49):

So what are some of those simple steps that we can take to help us be more secure, where we can do IP blockers or IP address blocking? So what those are going to do, they're going to help prevent malicious or unwanted IP addresses from accessing your data. The admin is able to manually add certain IP addresses to an allowed or blocked list, which we call access control lists. So this is going to ensure that those known attackers cannot view your user data or content via that LMS. The downside to this is that they can always use another IP address to work around that blocker, which is why it's essential to put other preventative LMS security measures in place.

Tanya Taplin, State Cybersecurity (00:31:35):

SSL certification. So the SSL protocol always encrypts the data that is transmitted so that only those end users logged in can read it. SSL provides that safe and encrypted environment that prevents other users in the same network from reading that data or those passwords. Password authentication, that's going to be the next one. So a good password policy that includes a combination of characters and numbers can make that stronger. Users should not use simple passwords for their accounts. A longer password is going to be a better password. Passphrase is going to be best. Those poor password choices often make those systems vulnerable and are one of the leading factors when an organization is compromised. Security, it is a process. There are some features that an LMS should have in order be secure, such as implementing group policies that lock accounts after three invalid attempts. This is going to help prevent those malicious actors from guessing or brute forcing a password. Not reusing passwords, that is going to be another best practice.

Tanya Taplin, State Cybersecurity (00:32:49):

Mobile security. So with more and more learners making that switch to their mobile devices, it's crucial that your LMS solution contains mobile security features. This includes data encryption, mobile user authentication, antivirus spam protection, or any type of endpoint security protection. I have endpoint protection on my personal phone. And after having it, I really would never be without it again. Just this last week, I was doing a schedule scan, it found that I had a leaked password from an account that I used at school years ago. I forgot that I even had this account, and I didn't even know what the password was. Right? So I can go in and I can fix those, but it's just a great way to have that extra security feature.

Tanya Taplin, State Cybersecurity (00:33:42):

Account registration. So for extra safety, your registration and signup process should require email verification in enabling security features like captcha and MFA or multifactor authentication. The administrator can easily restrict certain domains. For example, only school accounts from your institution should be allowed. You shouldn't be allowing students from other accounts. Those should be blocked. Remember, technology is there to solve security issues and protect the data in an LMS from cyber attackers. But it's important to give attention to the implementation of controls and design the process so that unauthorized access can be restricted. All right, next slide.

Tanya Taplin, State Cybersecurity (00:34:32):

So here are a few questions to ask any potential vendors, so if you're looking at implementing an LMS. The first one, how does your organization protect and defend against cyber attacks to ensure student information is protected? What information is a priority for your organization? A vendor should be able to easily answer this question. The salesperson, they may need to go and ask another person within the company, but they should be able to most definitely provide you with an answer. If not, that really should serve as a warning sign. Many organizations, they claim to be the safest out there with security measures that are going to be better than their competitors. When they make claims like that, make them prove it, make them show the validity to the assertions that they're making.

Tanya Taplin, State Cybersecurity (00:35:28):

Number two, has the vendor ever become a victim of a cyber attack or a data breach? If so, how? Has that vulnerability been resolved? So this is a question that should be asked to any vendor to determine if they are potentially a risky vendor. If they have fallen victim to a cyber attack, those next questions should be asked, is what changes have they made to properly secure their service or their software?

What did the vendor learn about those vulnerability risks? And what steps have been made to close those gaps? It's a right to you to have those questions answered.

Tanya Taplin, State Cybersecurity (00:36:11):

The next question, do you have a data security or cyber liability insurance? You may want to consider asking for a copy of their insurance certificate. Data is one of the most important assets your organization has. The widespread use of internet and technology has exposed higher education sectors to a wide range of cyber risk. Cyber attacks, they're a big business, and companies of all sizes are vulnerable to them. It's not just higher education. Those malicious actors, they're constantly looking for new ways to gain unauthorized access to your data. With new crimes emerging every day, data breaches are a question of when, not if.

Tanya Taplin, State Cybersecurity (00:36:57):

Does your organization include multifactor authentication? So multifactor authentication, it's a layered approach to securing your accounts. And data is one of the easiest methods that we can take to provide that extra layer of security. If you do not have MFA implemented in your current environment, I really highly recommend that you do that. And if you are looking for an LMS, that you're able to incorporate that, and that is one of the features.

Tanya Taplin, State Cybersecurity (00:37:28):

Are vulnerability tests run regularly? Vulnerability scanning is something that should be done on a regular basis. The only types of vendors that you want to be working with are the ones that recognize that security isn't ever evolving process. And they should be constantly be adapting to changes in the security environment.

Tanya Taplin, State Cybersecurity (00:37:51):

Is data encrypted? Data is being sent across the network, and it obviously falls into the wrong hands of people. So if you use a vendor, make sure that all of that data that they have, that they're capturing and that they're harboring is encrypted.

Tanya Taplin, State Cybersecurity (00:38:07):

Question number seven, where are you storing my data geographically? Where is your data stored in your infrastructure? And how do you transfer data? So if there is a breach at a facility in another state or country, you may be subject to that jurisdictions breach or privacy laws. So the best security in the world is worthless if it's being transferred in an unsecured manner. So make sure that that vendor has end-to-end encryption for those file transfers, especially if the data is containing PII. It's also not a bad idea to ask them about the destruction of data. If a vendor does not properly destroy data from decommissioned equipment, the data is needlessly put at risk. So ask your vendor about their data destruction processes. Next slide.

Tanya Taplin, State Cybersecurity (00:39:02):

All right. So here are just a few topics of discussion that you might want to have at your institution. So the first one here is, do you have your own in-house security team or is it outsourced to a third-party vendor? So it's becoming more and more common for universities to outsource their IT and cybersecurity to third-party service providers. This is a topic that kind of hits home for me in a lot of the discussions that I have with some of the higher education institutions that I have experienced with. Securing a campus can be expensive, we know that, but every university still needs to be involved in the decisions that are being made behind the scenes. Sometimes, colleges will transfer that risk that's associated with cyber to those third parties and take that stance that it's not their responsibility, or they hire it out, or it's the responsibility of somebody else. At the end of the day, that college is ultimately responsible. If a cyber attack were to occur, it directly affects that campus whether a third party is being paid to protect it or not.

Tanya Taplin, State Cybersecurity (00:40:15):

From another perspective, let's say that you have a supporter that on a regular basis donates a large sum of money to your institution. This supporter ends up becoming a victim of identity theft because its financial information is compromised in a security breach at your college. What would happen if you lose the support of that donor? Not only do you lose those future donations, but even worse, it damages that reputation of your institution. Or what if during a cyber attack or any type of attack all transactions for the last 20 years of your transcripts get compromised? Or what if student health data or athletic program data is leaked? Security breaches, they have long-term side effects. You take Lincoln College in Illinois, they ended up closing their doors. So it's very important for colleges to be involved in these decisions. It is your school that you're trying to protect.

Tanya Taplin, State Cybersecurity (00:41:16):

How often are third-party applications updated? So, as I mentioned just a few slides ago, it is very easy for an attacker to define current and previous vulnerabilities by just doing a simple internet search. Vendors should be providing updates to your systems on regular basis. And once those updates are available, they should be tested and implemented by your system admin.

Tanya Taplin, State Cybersecurity (00:41:43):

The next one, question number three is, is the principle of least privilege implemented? This is a common practice that we preach all the time. And quite honestly, I cannot stress it enough. I admit sometimes this can be a tough pill to swallow. It really can. Throughout my entire career, I've always had admin rights until I came to CISA. And then I found myself with, I couldn't install any software or anything on my laptop. It's not that I'm not capable, or I don't have the expertise, or I don't know what I'm doing, but it's because there's data that needs to be protected. And the same thing applies to higher education.

Tanya Taplin, State Cybersecurity (00:42:27):

The rule of thumb that I've always taught my security students is that users must have no more or no less than what they need to do their job. I have friends who work for businesses where everyone has administrator access to those laptops. I mean, that is just such a huge security risk. If one of them were to click on a phishing email, for example, they could easily expose that entire organization. So while sometimes it seems inefficient, security really needs to be the priority.

Tanya Taplin, State Cybersecurity (00:43:05):

And then have you identified cybersecurity gaps? If I were to ask you what the biggest risks are on your college campus, would you be able to answer that question? We first need to know what we are protecting and why we're protecting it before we can answer how we're going to protect it and what type of solution we're going to implement. Cybersecurity assessments, they're a great way to do that.

And as Dave mentioned before, we offer them here at CISA, and we offer them at no cost to our stakeholders. So it's a great way to find out what gaps that you have in your cybersecurity. There are also private companies that do offer them as well. And then just an interesting statistic here at the bottom of the slide that I thought was interesting. 75% of data breaches in K through 12 schools resulted in incidents involving vendors or partners. And I realize that is K through 12, but it's an interesting statistic anyway. And I just thought I'd mention it. Next slide.

Tanya Taplin, State Cybersecurity (00:44:16):

All right. So I want to briefly talk about strategy and actions to protect ourselves. Our overarching arching goal is to protect our schools for malicious actors, and we all have the same vision. Right? But first, we must accept the fact that our individual responsibility. We need to protect our data and information and make that a priority. We must also do our due diligence and not expect everyone else to do it. We need to educate ourselves about what to do and what not to do, and to report both internal and external cyber threats. Educational institutions need to provide learning opportunities for their employees. Having been in this sector, I know many times that this item gets put on the back burner. We all know that the budgets are tight in that education sector, but educating our employees needs to be a priority. And we really do need to do a better job of that.

Tanya Taplin, State Cybersecurity (00:45:16):

Second, operational and organizational teams who design and carry out any project involving technology, they must make protecting that critical data their responsibility. We need to get rid of that old mindset that only IT is responsible. Privacy and data protection needs to be at the front and center, and it's not just when we're talking about FERPA. Being in that education sector, I know how important FERPA is, but it's not the only thing that we need to be protecting. We need to protect the other privacy as well. So it needs to be included with everything. Third, our organizational leadership must accept the responsibility and provide those resources that we need to implement the framework and those policies, if we have any chance of being successful.

Tanya Taplin, State Cybersecurity (00:46:07):

And then the last comment I have is, I just wanted to reference a security study that I read earlier this week. It identified education as a perennial target for data breaches and colleges accounted for two thirds of the attacks on education. And out in this study, 130 higher educational leaders participated, and 40% of them overestimated their ability to recover from a ransomware attack, where they felt that they could recover from an attack in just under two days. In reality, just the downtime alone on average is closer to 21 days. So that's 21 days in a semester when every day counts, especially for those of you who offer accelerated courses where semesters might be five, six, seven, or nine weeks in length. So if you're down for 21 days, how is that going to affect your institution? So just something to think about with that. And with that, I'm going to turn it back over to Kathryn, and she can moderate the questions.

Kathryn Kerensky, Director, Digital Learning, (00:47:16):

All right. Thank you, Tanya. And thank you, David. This is great information. Thanks for providing the information and your contact information as resources for those who registered. We're going to turn to questions now. I have some questions drafted and there's some in the Q&A box. The first being from Matthew. When do you recommend having in-house security versus outsourced to a third party?

David Sonheim, Chief of Cybersecurity (00:47:40):

Yeah, I'll start off and I'll let Tanya jump on too. I started typing the response. Kind of where I was going is, although from a budgetary perspective or efficiency or feasibility, sometimes it makes sense to leverage a third party. I would say, it's not that third party won't do a good job, but I would say in generally speaking, someone who's part of our university family who understands our internal processes, understands the needs of the university, has got some passion for what we do as higher education, intuitively would take an approach to help secure and do that because it's the right thing to do. And unfortunately, when I go to a third party, that third party is going to do what's in the terms and conditions. Right? It's not that they don't care about the university, but I would surely think that someone who's got some equity within the university would absolutely make some decisions and the best interest of the university, just because they have a connection to it.

David Sonheim, Chief of Cybersecurity (00:48:48):

So I'll let Tanya kind of jump on that a little bit, but that would be my perspective, is even though you're going to get good qualified people and they're going to do good things as a vendor, always having someone internal within your best interests is probably always a good idea.

Tanya Taplin, State Cybersecurity (00:49:05):

Yeah, Dave is exactly right with that. It's not that we don't want to go to those third-party vendors. We can have something and they... It depends on your situation, right? Depends on the size of your institution, it's very, very hard to attract and retain people with those skills that are able to protect, but you need to just make sure you're on the same page. Right? If you're going to hire that third-party vendor, let them know upfront what your expectations are, what your priorities for the institution are. Just really have an honest sit down, one on one, so that everybody is on that same page and just so that your expectations are the same.

Kathryn Kerensky, Director, Digital Learning, (00:49:52):

Oh, great. Thank you. I have a couple of other questions that are sort of related. So I'll ask them in two parts. You mentioned those assessments that CISA can do, so how do institutions request those assessments that you mentioned? And then in addition, are there any suggestions that you have in terms of institutions obtaining some sort of training? So in addition to just having the audit of any gaps, just training that could be done practically to get an overview of issues to address for institutions.

David Sonheim, Chief of Cybersecurity (00:50:22):

Sure. Sure. So always happy to have folks reach directly out to Tanya or myself or your local cyber advisor, which can provide you a very detailed briefing on everything that's no cost, that's available. But I would say, in general, they kind of fall into two areas. The first one is, help you improve your program through reviewing your program, what's going on in your program, what activities, what controls. And those are the ones that we directly deliver as field staff. And so we're going to go out there, assess either that third-party risk or assess your overall program.

David Sonheim, Chief of Cybersecurity (00:50:55):

The second part that kind of goes with that, that CISA offers as no cost, is actually vulnerability scanning for you. So that's the easy one to get signed up for. Again, you can come directly to us or you can go to cisa.gov and you can type in their cyber resource hub, and it'll show you the entire list of services. But the easy one is basically no-cost, free cyber scanning. So we're going to scan, and they'll set up an agreement and it will all have the legal part of it. But the idea is to help identify some of those vulnerabilities or some of those gaps that maybe you don't have awareness of. And CISA does that at no cost. We do that from the infrastructure perspective, and we also do it on web applications. So, any of those websites or web applications that folks are interfacing with.

David Sonheim, Chief of Cybersecurity (00:51:41):

The reason we do those kind of differently is, when we look at physical devices that protect the network, we want to see what vulnerabilities exist there. When we look at a web application that was developed to actually provide input, or as I provide input, it takes me to Excel, that's a little bit different when we go to do the analysis of that. And so we have a little bit different solution that we say, "This value must equally exactly this, or it doesn't return anything." Sometimes thread actors like to probe those. And what they find out is that the coding, when they developed that web application, wasn't right, and the attacker knows how to put the wrong information as an input, which then actually gives them some level of presence. So those are the easy things that we do. We also do some further on pen testing, which is no cost, which is also part of that family.

David Sonheim, Chief of Cybersecurity (00:52:29):

And then to answer your question on the training, if you actually go to cisa.gov and cybersecurity and just type in training or incident response training, you'll actually see a whole set of no-cost webinars. There's some very detailed training in there for the actual cyber defenders. And then there's some general cyber training that's available there too. And most of that is all on demand. All you got to do is go in there and look at it and you can see when the schedule is for upcoming webinar. So Tanya, I'm not sure if I missed anything, but hopefully I got both those two pieces for you and Kathryn.

Tanya Taplin, State Cybersecurity (00:52:58):

No, I think you pretty much got that one. The only thing I would add to that is, in addition to the cyber part of it, also look at those physical security risks. When I was a professor, one of my favorite assignments that I did with students is, I've made them go walk around campus and just look at those physical security risks that are around there. It's amazing. There's fuse boxes that are just open. Right? Sometimes there's server rooms, wiring closets that are not locked. So things like that in addition. Those are just examples on how to better protect your campus in general.

Tanya Taplin, State Cybersecurity (00:53:39):

But when you have your in-service days, when the staff and faculty get together, just have some general cyber 101, like how do I make myself a secure password? Right? I found that a lot of people, they love to do summer and then the date of whatever year it is. Right? And it's just so easily cracked because it's just very, very common. So just things like that, how do you set up pass phrases and things. So, that's what I just wanted to add for that.

Kathryn Kerensky, Director, Digital Learning, (00:54:15):

Great. I think everyone would find those really helpful. And we have a follow-up question in the chat. Matthew follows up and says, right now that they do vendor assessments, review these various requirements, have cyber liability and a bunch of other contract requirements related to data breach, what else would you recommend? Or even just generally, are there any key strategies institutions should employ to mitigate risk or key terms and conditions? Dave, you mentioned that a little bit ago about conditions and terms, anything else that you would recommend there?

David Sonheim, Chief of Cybersecurity (00:54:50):

Yeah, no, I think Matt brings up a good point here. And if I'm reading kind of through the question, I guess, unfortunately some of that compliance stuff starts to get us in a position where we're doing activities to be compliant. Coming out of DOD, DOD is really good at being compliant but not so good at actually doing the actual hands-on controls to actually limit the real vulnerability or issues. So I would say, in general, as you do these or as you work with folks that do an assessment, it's got to be more of a holistic where we are doing these activities and we are doing them for very specific compliance reasons because there's requirements or government regulations or whatever the case is to meet them. But just because we're doing that, doesn't mean that we're really addressing this risk over here or this vulnerability or this piece that is actually helping us defend ourself better, or actually helping us control or limit the exposure of data better.

David Sonheim, Chief of Cybersecurity (00:55:53):

So, it's one of those things of, when they created the requirement or the control they put in place, meaning the regulation piece or the compliance piece, do they really account for everything and is that really ground truth? At the end of the day, we know that defending an organization, even if there's five layers of fences around Fort Knox, it still is difficult when we are all trying to do remote activities, we're trying to do remote learning. We have people coming and going. We have people internationally, it becomes a complexing problem. And so the idea is, we've got to create these layers and we've got to not do it because it's just a compliance piece, but because it actually helps us build resiliency. So Tanya, I'll let you add on to that one.

Tanya Taplin, State Cybersecurity (00:56:34):

I don't think I have anything to add. You answered that one perfectly.

David Sonheim, Chief of Cybersecurity (00:56:39):

I don't know about perfectly. Right.

Kathryn Kerensky, Director, Digital Learning, (00:56:44):

And with it being near the end of our time, I think we have time for one final quick question. And Tanya, you mentioned, in going through those questions, that institutions could ask some red flags. So I was wondering if either of you have any other gaps or red flags that institutions should be aware of when they're negotiating with vendors or third parties?

Tanya Taplin, State Cybersecurity (00:57:07):

I would just... Let's see. How should I answer that one? It kind of depends on how upfront they are with you. Right? I mean, you kind of can tell if somebody, depending on the question that you're asking them, if they're hiding something. So if they're showing you their vulnerability assessments, if they're showing you that they have a cybersecurity policy or insurance policy, things like that, those are going to be big things if they're not willing to show you where previous risks are because they should have fixed them. Right? They should be able to talk to you about some of those. So I guess it would just be how they approach your question, how they answer it. And I guess that's kind of how I would approach that. You're going to know if it's a local vendor. If there's other people that have recommended them, ask them for other customers that you could call and get reviews on. I mean, I've done that when I was in state government. When we would be searching for a vendor, we would require them to provide references for us. So you could do that as well.

David Sonheim, Chief of Cybersecurity (00:58:22):

Yeah. I'll be just real quick. I mean, if anybody's telling you they're perfectly secure, that is an alarming statement. The reality is, if you've been in this business more than five minutes, you know that it is a journey and there is no destination of perfectly secure. If they are demonstrating constant improvement, that is probably a vendor I'd want to engage with.

Kathryn Kerensky, Director, Digital Learning, (00:58:40):

Thank you both. I think those are great points. Thank you everyone for the great questions and to Dave and Tanya, for all the helpful information. I think it was a wonderful discussion with lots of great insights. I did see a question come up in the chat, so I just wanted to reference that and say we will get that to our speakers so we can cover that for sure. But now, I'm going to turn it over to Cheryl to close this out and highlight some additional resources and events.

Cheryl Dowd, Senior Director, Policy Innovations, (00:59:08):

Great. Thank you very much. Could you go on to the upcoming events please, Kathryn, I mean, Leah? Thank you. So yes, Dave and Tanya, you have provided such rich information. And as a matter of fact, between these two webinars, I know we talked last time during the webinar that this could have been a much longer series. And so I hope you don't mind we will be calling you because we would like to follow up on this sometime in the near future. So I hope you'll be willing to come back because we've really appreciated your work. We're also appreciative of our partner, WCET, in this event. And so I wanted to share here these upcoming events. There'll be a SAN Advanced Topics Workshop in September on succession planning for compliance continuity, and the WCET 34th Annual Meeting will be in Denver and October. So we hope that you'll look to these dates and the websites for each of these organizations to gain more information about how you can participate in the Advanced Topics Workshop and also in the WCET annual meeting. Go to the next slide please.

Cheryl Dowd, Senior Director, Policy Innovations, (01:00:10):

And so just finally, thank you again to our speakers and to our attendees today. You will find the recording, the transcript, and the slide deck available for you within the next few days on the SAN website. And we'll be sharing this with our WCET colleagues, so it'll be available through WCET as well. Thanks again, and we hope we will see you all again soon. Have a wonderful day.