READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS REMS TECHNICAL ASSISTANCE CENTER

Episode 28: The Importance of Collaboration in Cybersecurity and Risk Management

***#REMSontheAir* Podcast Intro (Recorded):** [00:00:00] Welcome to the *#REMSontheAir* Podcast, hosted by your partners at the U.S. Department of Education's Office of Safe and Supportive Schools and its Readiness and Emergency Management for Schools Technical Assistance Center. If you're an old friend, you know us as the REMS TA Center, your national school safety center.

Join us as we chat about key topics in school and campus safety, security, and emergency management with experts and partners from the field.

Janelle Hughes: Hello and welcome to another episode of *#REMSontheAir*. I'm Janelle Hughes, the project director here at the REMS TA Center, and today we are going to continue our conversation on cybersecurity planning and risk management for schools. I'm joined by my colleague Katie Barnett for this discussion. [00:01:00]

Katie Barnett: Thank you, Janelle. In episode 26, Chief Technology Officer Dr. Timothy Tillman joined us to explore high-impact strategies for preventing, responding to, and recovering from cyberattacks. If you haven't already, give that episode a listen at some point, as it's very informative. Today, we're going to consider the importance of collaboration in cybersecurity efforts. So, let's get started.

Janelle Hughes: Thanks, Katie. So recently, the REMS TA Center interviewed several subject matter experts in K-12 cybersecurity to learn from their expertise and their experience. So, we'll be learning from those interviews shortly. But before we do, I think we should spend a little bit of time reviewing research on the prevalence of cyberattacks on K-12 schools that we covered in our recent episode.

As we mentioned, the K12 Security Information Exchange's report, the State of K-12 Cybersecurity 2020 Year in [00:02:00] Review shows that schools of all sizes across all parts of the nation are receiving cyberattacks and that those attacks are really steadily increasing each year.

Katie Barnett: Common cyberattacks against schools include data breaches, ransomware attacks, phishing, denial-of-service attacks, Website and social media defacement, online meeting invasions, and business email compromise scams. The REMS TA Center's Cybersecurity Preparedness for Schools and Institutions of Higher Education Web page presents dropdowns with information on each of these threats and suggestions for prevention and mitigation strategies.

Janelle Hughes: That's right. So, whether it's developing a Cybersecurity Annex for your school EOP [emergency operations plan], performing and testing backups, implementing multifactor authentication, or working to minimize exposure to common attacks, your school deserves

solutions to prevent, protect against, [00:03:00] mitigate, respond to, and recover from cyber threats and their impacts.

So, let's turn now to our interview snippets from our cybersecurity experts to learn about the role of collaboration in implementing such measures.

Katie Barnett: Yes, the first expert we will hear from is Julia Fallon. Julia is the Executive Director of the State Educational Technology Directors Association, also known as SETDA. Julia works with U.S. state and territorial digital-learning leaders to leverage safe use of technology for learning and school operations. Julia also has worked for Washington's K-12 education agency and the Office of Superintendent of Public Instruction. She also has been a longtime member of SETDA's board of directors, even before her position as Executive Director.

Let's turn now and listen as Julia provides insight on what collaboration should ideally look like in the context of K-12 [00:04:00] cybersecurity.

Julia Fallon (Recorded): It should be ongoing and sustained. It shouldn't just be once a year we get together and we have a conversation and we check things off the box. It literally is a culture of making sure that the folks are at the table. And when you have a group that is coming together to do incident response planning, you want to make sure that you're representing all of your constituencies, including students in that—in there so that they can be good advocates for keeping your networks secure as well and reporting just things that they might see odd.

Often—people will notice that something's happening, but they haven't quite figured out what's, you know, like what's going on. Like, oh, it's like, "Oh, that's odd. That's not normally what happens." And then all of a sudden there's a bigger breach. So, it sort of likens to when you go to the airport and if you see something, say something, but you need to let people know that you're [00:05:00] actually even looking for those types of threats and whatnot.

So, but a collaborative model needs to happen. You have to have all of your stakeholders, again, like the front office leadership needs to be involved. Your school board needs to understand the risk, especially it could—it could have financial implications to a school's budget, you know, especially if people are paying ransom or you have to take down a network for a while, or you have to upgrade. It's a lot easier to think about preventative measures to mitigate risk than to have to, like, clean up after the fact.

So, collaboration is just important that there is a team of folks that are represented and they're talking to one another and they're thinking about how they're going through a school year, through a school year, through a school year. And that way you can make it part of the culture. It's a culture of—and I'm not talking about, like, where you're going to lock everything down. That's not the culture I'm thinking about. Like, I'm thinking about how you—people are all

understanding that they have [00:06:00] a responsibility towards keeping their accounts and their networks secure and it's—everybody plays a role in it, and everybody does a little bit of their part. Then, obviously, many hands make light work.

Janelle Hughes: Wow. It is so helpful to hear that collaboration is an ongoing effort and one that is of key importance to preparedness and prevention. As Julia suggests, when collaboration is part of the school culture, the entire school community is better equipped to leap into action and protect its assets when a cyberattack occurred.

Let's listen now to a snippet from Doug Levin, Cofounder and National Director of K12 Security Information Exchange, also known as K12 SIX. Doug has been involved in education and technology for more than three decades, holding executive positions within SETDA, the American Institutes for Research, and the National Association of State Boards of Education, among others.

Here [00:07:00] is Doug's take on collaboration within the K-12 cybersecurity context.

Doug Levin (Recorded): And then finally, the fifth thing that we think is really important is that school systems work together, whether that's in regional groups, state associations, or in national organizations, whether they are with the Federal government or private or nonprofits or associations.

This is something that is going to be a significant challenge for many school systems, particularly those that are smaller and more rural. The thing to know is that this is something that you are not facing alone, right? And so, reach out to your colleagues, learn about what they're doing. You're not in competition with other school systems with respect to cybersecurity. Be generous in sharing your advice and be active in seeking it and in giving it as well.

Katie Barnett: I love this. What a great point that school systems are not in competition with each other and can instead collaborate with each other against this [00:08:00] issue. I think it's easy for schools of all sizes to think that they're alone in these types of struggles, but joining with other schools and groups across all levels can forge the partnerships that we need to succeed.

Our next subject matter expert is Ray Girdler, Director of Data Use and Privacy at the Arkansas Department of Education. Ray has served in multiple roles at school and district levels over the years. He provides direct support for K-12 schools and school districts in maintaining security and data privacy utilizing data and other technical supports. Here's what Ray had to say about what ideal collaboration structures for school cybersecurity efforts could look like.

Ray Girdler (Recorded): I don't think—when we talk about our internal response team, no one person is an expert at everything. And when we find a district that's under attack, I think one of the reasons why we feel like we have a lot of resilience and confidence is not because that our team is so strong, [00:09:00] but how our team is networked between the 15 folks that we have serving on this team. They all know someone in the K-12 environment that can assist us in some way, to help us get to where we need to be. And I think that's probably the most important thing, whether it be the runbook that we talked about earlier or on your COOP [continuity of operations plan].

When we go in after the district's been under attack, no matter—because it happens to the strongest districts, it happens to the weakest districts. And so, when we go in, it doesn't matter how strong this tech was before the event, this is probably their worst day and stress has set in and panic sometimes sets in. And time and time again, we show up and they're calling one of our people and they're just, they're just, "Tell me where to start."

And it's like all the inst—all the knowledge that they had in this moment of crisis, sometimes [00:10:00] just kind of alleviates. And that's where, one, having a written plan is so important, but in that plan, making sure that you have all your points of contacts kind of listed off there and what resources that you have available to you, because at the end of the day, you never know which one you're going to need. And it is the network of people from your vendors to your people that are working at your state to who might be working at your education service cooperatives to nearby districts. I mean, these are the people that are going to help pull you through the crisis. And this, I mean, it's—the stronger your network is, the stronger your resilience is to an attack or to recover from an attack.

And so just encouraging techs in tech communities to really build out that network so that you know who you can call on when. And we've called on all those, from our vendor partners to, I mean—but it's even the kind of a step level for—even from the state. I mean, we try to establish relationships with CISA [Cybersecurity and Infrastructure Security Agency] [00:11:00] before an event. We try to establish contacts with the FBI before an event. These are relationships that you want to have in place—maybe your local law enforcement—these are all relationships that you want to initiate before an event occurs. And I tried to establish: the more you can handle on the front end, the quicker you'll be able to recover on the backend and the people really make a difference.

Janelle Hughes: It's so helpful to hear those differing perspectives. And as Ray mentioned, collaboration will make you stronger in practical ways, such as with backups, as well as in understanding what to do in times of crisis. When it comes to cybersecurity, schools and school districts can't afford to be lenient. I'll definitely be keeping these practices in mind as I think through this topic going forward.

Katie Barnett: When it comes to the helpful partnerships that Ray mentioned, the U.S. Department of Education and its REMS TA Center have multiple resources and training opportunities to support this topic. [00:12:00] Improve your cybersecurity posture and prepare to prevent, respond to, and recover from cyber threats by visiting our cybersecurity preparedness Web page or downloading one of our cybersecurity training packages.

You may also want to check out our fact sheet on building a Cybersecurity Annex or our Cybersecurity Considerations for K-12 Schools and School Districts online course.

Janelle Hughes: Yes, the REMS TA Center is happy to serve as the first stop for you in your cybersecurity efforts. You can follow REMS TA Center on social media, bookmark the REMS TA Center's *#REMSontheAir* hashtag, and use *#REMSontheAir* on X if you are addressing similar topics.

As always, reach out to us if you want to learn more or just have questions related to today's topic. You can give us a call at 1-855-781-REMS, or 7367, to pose questions that can possibly [00:13:00] be featured on future podcast episodes.

Katie Barnett: And also, remember you can email us, too, at anytime at info@remstacenter.org. You can also join our mailing list there to get timely information on webinars, Web chats, and other virtual opportunities to learn and share.

Janelle Hughes: And of course, access additional *#REMSontheAir* Podcast episodes and share this one with your colleagues and community partners by visiting the *#REMSontheAir* Podcast page on the REMS TA Center's Website and click the share tabs that appear on the screen.

Thank you again and so much for being with us here today.