READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS REMS TECHNICAL ASSISTANCE CENTER

Episode 32: Reframing Expectations: The Role of School Board Members in K-12 Cybersecurity

#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: Welcome to another episode of the *#REMSontheAir* Podcast. My name is Janelle Hughes and I'm Project Director here at the REMS TA Center. Today, I'm joined by my colleague Katie Barnett to consider another critical aspect of K-12 cybersecurity.

In recent [00:01:00] cybersecurity episodes, we've touched on the importance of collaboration, initial action steps, and high-impact strategies that K-12 schools can use to prevent, respond to, and recover from cyberattacks. Today, we're going to take a different approach and focus on an aspect of cybersecurity that, while of utmost importance, may be just far enough outside of the box so as to be overlooked. And this aspect is the role that school boards play in cybersecurity at the school level.

Katie Barnett: To help address this topic, we are pleased to have Dr. Timothy Tillman back on the show. As you may recall from his last episode, Dr. Tillman is the Chief Technology Officer for Virginia's fifth-largest school district. He is also an excellent speaker and has been part of many REMS TA Center live and virtual trainings this year. Let's hear from Dr. Tillman now. [00:02:00]

Janelle Hughes: Hello, Dr. Tillman, and thank you so much for joining us today. We so appreciate you being here and truly cannot wait to learn from your expertise.

First, I'd really like to talk about something that comes up commonly in schools. When a cyber incident happens, most staff and faculty seem to think that they should just let IT handle it. But I know I've heard you say before in our trainings that this way of thinking can really cause problems for schools. Can you explain that a little bit for us?

Dr. Timothy Tillman: Sure. So, I think that in a typical school district, cybersecurity is the domain of the IT department, right? So, when an event happens, of course administration and the boards are looking to the IT department for answers. They're looking to them to kind of describe the problem, [00:03:00] you know, describe how big it is, what it affects, and how to get out of it, right? But what my philosophy comes down to is that the board should have a better understanding of what those impacts actually mean and how much their own IT department can handle an incident.

An IT department is trained to be the superhero in the room, and they are *not* trained to admit when they have a vulnerability. They are *not* trained to say, "We need help." And the default action of "Don't worry, we have it under control" is very easy for a board to accept and say, "Oh, great, no problem here," right?

And I think that the board as a governing structure needs more [00:04:00] understanding, not necessarily need to direct the activities, but needs a better understanding of what is actually occurring during a cyber event. As they become more and more prominent and occurring more often, a board should have confidence in their ability to understand and not have to completely rely on the local IT team. And that is really where the shift in philosophy comes.

Janelle Hughes: Thank you so much for sharing that. I think, you know, that shift in philosophy, as you noted, is so important, you know, really reframing those expectations around who needs to be fully involved in the process. So, thank you so much for sharing that.

Katie Barnett: Dr. Tillman, I've also heard you spoke at our trainings before about the important role of school boards in actually creating a really strong K-12 cybersecurity posture. Can you tell us [00:05:00] more about the actions and activities that they can implement to do this?

Dr. Timothy Tillman: So, a school board really does have the ability to set tone for the school district. They have the ability to, as a governance structure, they have the ability to set policies and to set expectations that then an administration or an IT department has goals and they have a roadmap ahead of them that makes it easier for them to establish or maintain a cybersecurity program.

If the IT department is left on its own completely, they're gonna focus on what they feel is important. And that may include cybersecurity, that may not include cybersecurity. It may include, you know, the things that they find important may be more technology services–related [00:06:00] events or, you know, just keeping the lights on, right?

But the governance structure is there for a reason. It's there to provide that roadmap. And I feel like school boards in general have not necessarily been providing that roadmap for something as critically important to operations of every single department of a school district as cybersecurity is.

And it is, as we mentioned in the first question, it is not something that can just be handed to the IT department and say, "You go handle it." More stakeholders have to be involved. More voices have to be heard. The IT department cannot be the ones who strategize, implement the strategy, verify their strategy, audit their strategy, and then try to figure out also how to pay for it within their current operational budget, right? They [00:07:00] need help, and, again, as I mentioned, they’re not necessarily trained to ask for that help. They’re trained to be superheroes, they’re trained to be the people who calm others down during emergencies and say, “Don’t worry.”

And, again, that is the, that is the philosophical change of if I can get more school board members to understand that this is a critical area for them to monitor and for them to be aware of, that things will be better in the long run, things will start to make more sense, you know, budget justifications will make more sense and reporting will make more sense and there won’t be so much fear around cybersecurity that makes people say, “It must be someone else’s job.”

So again, we have this old mantra from, you know, from the—I heard it first— and as early [00:08:00] as 1994, right, that “Cybersecurity is a shared responsibility.” Well, it is, and everybody has to have their little piece of the puzzle, and it is just too easy to say, “Oh, that’s an IT thing, don’t worry about it.”

Katie Barnett: This is so great. Thank you for sharing that. I—as I was listening to you, I couldn’t help but think, it almost sounds like school boards could have the role of, like, an influencer in how they’re guiding. So, I kept getting the picture of if school boards really get the mindset that what they do really sets the tone, it sets the expectation. They’re kind of the trendsetter for the entire school realizing this is so important. Then IT is freed up to function as the arm. But I’ve never thought of it in terms of that.

Dr. Timothy Tillman: Absolutely. [Cross talk] I think that’s absolutely right, and I spoke to some school board members in my state earlier this week, and I said, [00:09:00] “Look, you have the ability to be the cheerleader, you have the ability to set the tone and say, ‘You know, this new multifactor authentication that we’ve implemented makes me feel so much safer,’” right?

Katie Barnett: Mm-hmm.

Dr. Timothy Tillman: Instead of it being the IT team having to push those efforts and support them and justify them and in some cases just force it, right, like, “We’re going to do this, whether you like it or not.” The school board has the ability to say, “Look, we understand that these changes that we’re making are different and they are—sometimes they take a little bit more time to occur, but we believe, we believe as the school board that this is making us bigger, better, faster, stronger, and that we support this, right? We support what is going on here, and, you know, I personally—I’ve been doing it for a little while and I don’t find it that bad.” You know, those kinds of things that they can do, and they already do those support [00:10:00] efforts for other things that happen in the school district. They’ve just never really been asked to do it for this particular topic.

Katie Barnett: Yeah, that is so fascinating. I know I definitely didn't even realize I had some of those expectations towards IT, so, this is, this is so enlightening. Thank you so much.

Dr. Timothy Tillman: Mm-hmm.

Janelle Hughes: It really is enlightening, and I agree, Katie, in kind of thinking about some of those expectations that we have of IT teams. One of the terms that we hear a lot about in the context of cybersecurity posture and preparedness is "outside-vendor risk." So, in thinking about the role of the school board as this cheerleader or influencer, would you say that school board members have any responsibilities related to helping to mitigate these outside-vendor risks or prepare, you know, preparing the school community for them? And if so, what actions should they be helping to take to address them? [00:11:00]

Dr. Timothy Tillman: So, I think this is really one of their most critical aspects of governance. In that the school board has the ability to set policy (or, again, like, you know, I understand the board doesn't write their own policies necessarily, but the administration can write policies that the board supports) that set the tone, that say, "You will not work with a vendor who does not provide you with security information" or "You will not work with a vendor at a procurement level that has had a data breach within the last six months," right?

And I'm just throwing things against the wall. These are, these are kind of extremes, but they have the ability to say, "You must vet these vendors, OK?" It's not just, "Oh, well, they're number one in the space, so that's who we're going to use" or "They have the lowest price, so that's who we're going to use." That cy—that cybersecurity component, that data privacy component [00:12:00] has to be built into policy so that there is yet another series of checks and balances against what data we're giving those vendors. How are they then protecting that data on our behalf?

Now, I will be the first to admit, the IT department is probably already doing a lot of that. But this is, this is more about making sure that that more people are aware and that nothing slips through the cracks. So that's why you create a policy. You create the board policy so that it's not a, it's not an individual decision of "Oh, we don't need to vet that one. I know that company, they're fine," right? And we get a lot of that. We get a lot of requests for "I used this software at my last district. They used it, so we should use it," right? Well, they may have had different criteria than we have for what we consider an acceptable risk.

And that, again, that lends itself to the board as a [00:13:00] governing body must decide what acceptable risk is, and they must decide what their risk appetite is. And those are, those are terms that we use in cybersecurity to kind of get everybody on board to say, "Nothing is 100% safe. Are you willing to share data with this company that you know has mishandled data in the past?" right? Now, they say they've corrected all of their mistakes. They say they are better than they were, but are you willing to accept the risk that we could expose student data, staff data, employee data, whatever, to this company, and we don't know, we just don't know. Are we willing to accept the risk, right?

But the board is the one who ultimately is responsible for that data as a governance structure. When the, when, if there is a data breach, if there is a problem, the public is going to look to the [00:14:00] board for answers. The board members are going to be in the hot seat. They are going to be the ones who have to answer questions about "What did you know? Who knew it? And when did you know," right? Those questions of "Why did you work with this company? It was pretty obvious. They had a breach a year ago," right? So that is where that risk appetite comes in. That gives those board members the confidence to say, "Listen, we understand that there were problems in the past, but we believed as a board (and the IT team agreed, and the administration agreed) that we were—that we had faith in this company and we could move forward with them," right? That's the shared responsibility part.

And when it comes down to it, if the board puts these guardrails in place, everybody will then use those guardrails, and it becomes a smooth highway. If you don't have the guardrails, cars are all over the place, right? And it just makes [00:15:00] a lot more sense to establish that foundation in the beginning and to make sure that especially board members are aware that *they* are the ones accepting risk, not the IT department, and that is a burden of being the governance structure.

Janelle Hughes: That's really powerful. And so, I—my follow up question is, so in looking at, you know, putting these guardrails in place and in looking at setting up the policy parameters, what do those conversations then between those board members and IT directors, IT professionals look like? Or should school boards consider having an IT professional as, you know, a recurring presence? You know, how is the board getting the knowledge and information that they need guardrails up? And to, you know, continually update and maintain those policy parameters. What does that process [00:16:00] and kind of two-way communication look like?

Dr. Timothy Tillman: So, I have a three-pronged approach. And I'll see if I can remember all three while I'm speaking. [Laughs] So, the first prong is lean on your IT department, right? None of, none of my, none of my preaching, none of my teaching, none of my philosophy involves not trusting your IT department. What I am saying when I mentioned IT departments is that they need help and that they need guidance from the governance structure to say, "What do you want us to do? Once you establish those rules, we will implement it. We will make it awesome. We will polish it. It will be perfect. It will be exactly what you asked us to do." That's the power of the IT department.

So, in the beginning, when the board's knowledge about current environment and "What should we do? And I [00:17:00] don't even know where to begin." That's the first step to say, "Dear IT department, can you explain your view of what we should be doing?" Right? And I guarantee you they have opinions. I guarantee you they have, they've just been begging for someone to ask them. Because they have been living this. The part of that prong then becomes the board establishing policy and guidance that then holds the IT team accountable.

And by that accountability or, excuse me, that accountability gives the board, the board confidence that what they said need to occur is actually occurring, right? IT teams don't mind accountability. It, again, it gives them a goal to work toward. [00:18:00] If they don't have the accountability, they just do the best they can every day and they just get through it.

The second prong is that the board members themselves need training, and they need to understand some basic vocabulary. They need to understand some basic concepts. And they need to know what questions to ask and when to ask them. And that is something that they're probably going to have to work with an outside vendor to establish some basic knowledge, to run through things like, "What do we do if there's an incident?" Right? What does incident response look like for a board? Because, again, in that moment of panic, in that moment of "We're under attack," they need confidence, they need confidence to be able to talk to the public, to talk to the press, and to talk to their internal teams.

They are not the ones running the incident. And [00:19:00] that's not, I mean, I don't want anyone to confuse that. They're not going to be in charge of that, but they need to have the confidence to be able to have the conversations and not just always be in that position or that seat of "I guess everyone around me knows what they're doing, and I'm just, I'm just taking it in," right?

So, my suggestion has been that the board should engage in annual training that keeps them up to date, not just on vocabulary and structures and in current state of affairs, but also teaches them what else is occurring in the country, what other school systems are seeing, what kind of incidents have happened out there, and can you ask questions of your IT team that says, "Listen, this happened in California" or "This happened in Wisconsin," "What are we doing to make sure that doesn't happen to us?" That is the kind of question that a governance structure needs to ask, whether in closed session or not, that said—that gives them the confidence to know that IT team is being held accountable [00:20:00] to the rules that they established earlier.

The third prong is that I believe a board needs an expert resource that they can call or talk to or email for any reason whatsoever. They can ask their silly questions, their dumb questions. They—not that they have those, I'm saying, like, *they* would classify it that way—they can ask any question they want to about cybersecurity because they may not feel comfortable asking their internal teams those questions. So, they need an outlet, they need a resource and maybe not an outside vendor that they have to pay to do that.

So, it has been my advice in the past that the board reach out to their local FBI office to establish a relationship with an agent that works in cybersecurity. It has been my experience that the FBI agents that are assigned to cybersecurity (especially if you have a local office that is assigned to school cybersecurity, which we are lucky enough in my district to have), those agents are [00:21:00] anxious to have these relationships. They would love to talk to you about your fear, about your concerns, about, you know, anything you have because it sharpens their own skills, and it sharpens their own awareness of the environment.

You—in our state of Virginia, we also have—our state police has a cybersecurity division that they call the Fusion Center. They have the exact same kind of environment as the FBI does, but we establish a relationship with a police officer, a state police officer, so that we just have that other resource to say, “Hey, this is what’s happening” or “This is what I’m concerned about. I can’t find answers online. I feel embarrassed to ask my staff this. What can you tell me real quick?”

And, again, that is all about building confidence, and it’s about building an awareness that the board has never really been asked to do in the past, and I feel that it’s important [00:22:00] that they start down that path of taking cybersecurity out of the realm of “Somebody else must be doing it” to “I not only know that we are doing it, I know that they’re following our rules and that there is a proper structure in place to help keep our data safe and to keep our students safe and staff and employees and families and everybody to have trust in us.” And that’s kind of the whole picture there, right, of those three things need to occur in order to bolster that cybersecurity at the top.

Katie Barnett: Dr. Tillman, thank you so much for sharing that three-pronged approach. That really sounds like a super great way for school boards to grow from where they are now to where they need to be and possibly in ways they didn’t even imagine were possible to protect their schools.

Kind of jumping off of that, [00:23:00] now that we’ve talked about school boards, what are your suggestions for how school communities as a whole can and may need to adapt to more realistic expectations about cyber vulnerabilities and their responsibility to help with them?

Dr. Timothy Tillman: I think that as a school board matures in their awareness and their ability to speak the language and their ability to hold others accountable, I believe they can also do some outreach to the community. And I think that that can be done through advisory boards, that can be done through public comment, it can be done through any vessel that they already have. But there are—in every community, there are others who have expert opinions and there are others who can provide valuable input. And as an IT leader myself, I am [00:24:00] sometimes hesitant to ask for additional input, but usually I’m happy at the end when I get it, right?

So, the board can establish, again, can establish those rules that says, “You will do this,” right? “You will have an advisory group”—or a steering committee or whatever it is that just really gets the community not necessarily involved but aware, right? The community needs the same level of confidence that the board has. They need to know that when I provide my child’s demographic data and my child’s medicinal data and my child’s discipline data that you are not mishandling it by negligence, right? They’re not going to need to know the ins and outs and what framework do you follow and, you know, what does the exact rule say, they just need the confidence.

It’s the same confidence that they would have to say, “I [00:25:00] trust that when I put my kid on the bus, I know where that bus is going today, and I know that they never veer off the track. I know that they don’t stop at 7-Eleven real quick to get a drink. I know they don’t do those things because there are rules in place.” That’s the same level of confidence they need for data and for the activities that their student does on the internet. And I venture to say a lot of them don’t have that. And it’s very easy to get in front of communities and say, “We’re doing the best we can. What do you think we should be doing differently?” It’s not an admittance of failure. It’s not a vulnerability. It’s “We believe that we are doing the best we can,” right?

So, communities really only act when they’re asked to in most cases like this, right? If it’s something that is, that is charged in the community, of course, they will bring it to the board’s attention. But if the board specifically asked the community for [00:26:00] input around cybersecurity policy, around best practices, around, you know, configurations or anything like that, there will be people out there who voluntarily say, “Listen, I work in this field and here’s what I think you should do” or, you know, any example like that. So, when it comes down to it, the more voices you have, the better. Those voices are not directives. They are just voices. They are just people or thoughts that help the IT team brainstorm more or say, “You know what, we didn’t really think about it that way.”

And, as I said in the very beginning, IT teams are not necessarily trained for that. They are trained to be the expert in the room and that “Whatever my brain says is the answer.” And that is not, again, that is not a [00:27:00] failing. I love my IT teams across the country. It’s just that’s the way we are. We are, we are just trained that way. And it’s hard for us sometimes to come back and say, “You know what? That person who spoke at the board meeting last night, they were actually right, we need to make a change today.” And that’s very powerful. And it makes everybody feel better to say, “Gosh, we really learned something, and we made a change based on a public comment or based on a parent concern and now we’re better, we’re stronger,” and everybody down the line from the board to the administration, superintendent, everybody will just feel like “Gosh, that was, that was really great, right? What do we do next? What’s next?” And that’s, you know, that’s gold to me. It’s fantastic.

Janelle Hughes: This has really been such a powerful conversation. And I think there are so many key takeaways, you know. We talked about the importance of school board [00:28:00] members engaging in training so that they really know the language and, you know, involving multiple voices and they are really like the perfect forum to do that, voices from the community, you know, from community partners. And that's going to really, you know, support that situational awareness as you said the more voices you have, the better, and then taking that preventative action. And, you know, as you said, understanding that, "Yes, we can start today."

So, I think to close things up, if you could make an ideal school in which school boards and IT staff work together to really protect the school from cyberattacks, what would that ideal structure or relationship look like?

Dr. Timothy Tillman: It would be a structure that everyone understands and that everyone has had a part in creating, and by everyone, I mean each different stakeholder group has had some sort of [00:29:00] input into that. It would be a user community within the school that understands that sometimes cybersecurity can slow you down a little bit, right, but it's important.

I understand that doing things like locking screens automatically or making people log in, multifactor authentication, those are things that slow you down, and from a teacher standpoint, it's a burden to instructional time, right? But when we build that understanding of the reason why we're doing this, we don't, we don't just do these things just because, right? There is a real tangible benefit to these things, and it—there's just no way around it, right? It just has to be done because it's the best we can possibly do right now. That community also is one that accepts those [00:30:00] changes and that is excited to be in an environment where they can feel safe and where they know the kids are safe.

So, it is, it is important to remember that cybersecurity is not just logins and passwords. It is not just the gatekeeper. Cybersecurity encompasses everything that we do when data moves from one person to another, from one system to another, that is cybersecurity. When data is collected on anything as simple as a, as a fieldtrip form, that is cybersecurity. And when everyone has a shared understanding of what that means, they start to treat all of that differently.

I have, I have often used the idea that people are so—or people in our schools are so good at knowing their [00:31:00] jobs that it is second nature to them. If you are standing in a bus loop when kids are boarding buses, if one kid strays off somewhere, you will see seven adults wander and find that kid and notice immediately that they wandered off, right? That is just, it is, it is inherent in them, it is second nature in them to go "No, no, no, no, no. You're supposed to be over here," right?

That is the kind of power that they could have with cybersecurity from—for their portion of cybersecurity: to say, “Wait, wait, wait. We shouldn’t be sharing that data,” “We shouldn’t send that through email,” “Did I lock my computer when I walked away from it? Oh, gosh, let me go check real quick,” or “Should I let this person in the building today? I don’t see any ID,” I don’t see this, I don’t see that, you know? That’s the kind of second-nature mentality that would make a school community and school environment incredibly powerful and much more safe. [00:32:00]

Katie Barnett: That’s so neat to hear because I think we can think cybersecurity is very complicated. And it’s true, maybe not everyone on the staff understands how the different attacks are created or come to be, but doing things like making sure that we’ve logged out of a computer system, that’s something that everyone can do. That’s really neat that if everybody knows their role and joins in the effort and understands how important this topic is that that can be enough to really create more power and protection in schools.

Dr. Timothy Tillman: I just want to add to that, that that culture, that culture change within the schools starts at the school board level.

Katie Barnett: That’s amazing, just the influence they can have and knowing that that is part of their role when it comes to cybersecurity.

Dr. Tillman, we thank you so much for your time today. This was incredibly [00:33:00] helpful, and I think this information is really going to impact this space. Thank you for all that you’re doing to support cybersecurity in our schools.

Dr. Timothy Tillman: Thank you. I appreciate it.

Janelle Hughes: Well, Dr. Tillman certainly gave us a lot of helpful information today. To learn more, you can visit the REMS TA Center Website and access our cybersecurity and K-12 cybersafety resource pages, as well as our free online course Cybersecurity Considerations for K-12 Schools and School Districts.

Katie Barnett: And if you would like the REMS TA Center to come and do a live training for your audience at your location on the topic of cybersecurity, you’ll find our training application request forms on our Website as well. All of our trainings are free of cost to you.

Janelle Hughes: Don’t forget that you can also join our mailing list or connect with us at any time on these and other school emergency preparedness topics by emailing info@remstacenter.org. [00:34:00] Our mailing list is where you’ll get updates on our newest webinars, Web chats, podcast episodes, our monthly newsletter, and other virtual opportunities to learn and share. You can also reach us by giving us a call at 1-855-781-7367.

Katie Barnett: Social media is also a great place to connect with us. Visit X and bookmark the hashtag *#REMSontheAir* or follow our feed @remstacenter.

If you can't get enough of the podcast, you can access our full library of episodes by visiting the REMS TA Center's podcast page. We even have a share button so you can easily share episodes with your colleagues.

Janelle Hughes: And if you ever have an idea for a future podcast episode or a topic that you'd like to hear discussed, just let us know. You never know if your idea may be the inspiration for a future episode. For now, have a great day, stay safe, and remember, cybersecurity [00:35:00] is a shared responsibility.

Katie Barnett: Bye everyone!