READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS REMS TECHNICAL ASSISTANCE CENTER

Episode 30: First Steps to Improve Your School's Cybersecurity Posture

***#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 *#RemsontheAir*. I'm Janelle Hughes, Project Director here at the REMS TA Center. I am so thrilled that today we will continue our discussion on cybersecurity planning and risk management for schools with guidance from subject matter experts, Doug [00:01:00] Levin, Julia Fallon, and Ray Girdler. I'm joined today by my colleague Katie Barnett as we explore this important topic.

Katie Barnett: Thank you, Janelle. This episode augments what we've covered in episodes 26 and 28 on cybersecurity planning and risk management. So, for those of you who are just tuning in now, be sure to give those a listen also.

Here at the REMS TA Center, we are passionate about helping schools and school districts keep abreast of current topics and threats, and I think we can all agree that these days, cybersecurity is often at the top of the list.

Janelle Hughes: You're so right, Katie. Recently, the REMS TA Center interviewed several subject matter experts in K-12 cybersecurity to learn from their expertise and experience. We'd like to hear more from the interview snippets that we explored in our last episode. While we explored the role of collaboration last time, today we will consider initial [00:02:00] practical steps that schools can take to improve their cybersecurity posture.

With a topic as important as this, it's often easy to get bogged down with the severity of issues or the technical jargon. But what can schools do today to improve safety if they don't know where to start?

Katie Barnett: What a great topic, Janelle. Thankfully, the subject matter experts we interviewed had a lot to say about this. Let's hear from them now as they answer the question: What should a school focus on first if they do not know where to start? After hearing from each speaker, we will compare notes and compile a short hit list of important steps that schools can take today.

Our first speaker is Ray Girdler, Director of Data Use and Privacy at the Arkansas Department of Education. As you may recall from our earlier podcast, Ray has served in multiple roles at school and district levels over the years. He provides direct support for K-12 [00:03:00] schools and

school districts in maintaining security and data privacy, utilizing data, and other technical supports. Let's hear what Ray has to say regarding first steps.

Ray Girdler (Recorded): A lot of the things that schools can do are low cost or no cost. And these include things like multifactor authentication or, you know, just going through your audit. Audit your active directory and change your permissions so that you can start practicing "principle of least privilege." Start removing those admin credentials from accounts that don't need admin credentials. Those are some very simple things that you could do on both sides of—on the reactive side or on the proactive side.

You need to make sure that you have clean and tested backups and that one of them is offsite. If you don't have a COOP [continuity of operations plan], you need to get a COOP. If a COOP seems overwhelming, go check out a runbook. Establish some key contacts that you have. That is a—put together a [00:04:00] network map, or what we call them a "site notebooks," so that if someone wants to come in, they could assist you. If there was a place to start, that'd be a place to start.

What we hear over and over again, when we started doing a lot of this work is—our techs were like, "Stop telling us what we have to do to react. It's like, I never want to be in that position, so what do I need to do to prevent?" And so many of the things that you can do in recovery, you also do to as a preventative measure.

And one of those things is if you haven't done one, strongly consider doing a vulnerability test, do a vulnerability scan to find out where you're weak, that's a really good place to start and start prioritizing. If that seems too overwhelming, do a—go find a self-assessment. There's self-assessments everywhere. CISA [Cybersecurity and Infrastructure Security Agency] has one, K12 SIX has one. Go do a self-assessment, and that'll help you prioritize a list of things where you can start getting healthier.

And again, they sound simple. They may even sound repetitive to folks who have [00:05:00] heard some of these conversations, but if I go back up to the things that we've seen over and over again, I think sometimes people mistake simple for effective, and the fundamentals matter.

Janelle Hughes: Wow. That is so helpful to hear. So, according to Ray, setting up multifactor authentication, completing an audit and protecting credentials, backing up information, creating a contact list, and a self-assessment, and establishing a continuity of operations plan are all important steps. For those unfamiliar with COOP, or continuity of operations planning, we will touch on that briefly toward the end of the episode.

For now, let's hear from Julia Fallon as she answers the same question. Julia is the Executive Director of the State Educational Technology Directors Association, also known as SETDA. As you may recall from our past episode, Julia works with U.S. state and territorial digital-learning leaders to [00:06:00] leverage safe use of technology for learning and school operations. Julia has also worked for Washington's K-12 education agency and the Office of Superintendent and Public Instruction and has also been a long-time member of SETDA's board of directors, even before her position as executive director.

Julia Fallon (Recorded): So, I think to get started, you would try to figure out what you already have in place and then think about where you want to go with it. Everybody should have an incident response plan, is one of those things, so that could be an easy—an easier goal to try to put together. Like, what would you do if there was a breach, if there was an attack on your network? I think, it's always maybe doing a needs assessment and thinking about—there's lots of great resources out there by CoSN [Consortium for School Networking] and some others where you can think about your needs assessment of where you actually are. You [00:07:00] need to figure out what your baseline is, where you are starting from.

Katie Barnett: I love how Julia put that: start by figuring out what you already have in place and then work from there. Having an incident response plan and performing a needs assessment are great steps that schools can take right away to improve their cybersecurity posture. Let's hear one final snippet from Julia about an initial helpful step to take.

Julia Fallon (Recorded): Knowing how to talk to non-tech people. So, if tech folks are here, you really have to understand how to be able to communicate to non-tech people what you're talking about. So, for example, you know, again, why is K-12 a target?

Just helping people understand the importance of the fact that we are keepers of a lot of very sensitive personal information. And that is what often attackers are after.

Katie Barnett: Hmm! Taking time to learn [00:08:00] common cyber threats and jargon to be able to communicate those to non tech staff, faculty, and stakeholders, giving everyone a common language—it's a great way to begin strengthening systems and getting everyone on board with current and future cybersecurity measures. People often won't care about what they don't understand, so this insight from Julia is very helpful.

Last, let's turn to Doug Levin to see how his recommendations align with those of our first two experts. Doug is the Cofounder and National Director of K12 Security Information Exchange, also known as K12 SIX. He has been involved in education and technology for over three decades, holding executive positions within SETDA, the American Institutes for Research, and National Association of State Boards of Education, among others. Doug is the mastermind and

creator of the K12 Cyber Incident Map and is one of the most influential and sought out individuals to speak about education technology and research.

Let's [00:09:00] hear from Doug now as he answers, what should a school focus on first if they do not know where to start?

Doug Levin (Recorded): So, there's a number of things that we believe are critical for the K-12 sector writ large to put in place to better defend school systems and school communities from these emerging cyber security threats.

The first, we think it's critically important that school systems share more information with each other, with policy makers, and with law enforcement when they are victims of cyber incidents. This is not something that—this is not an issue that is just affecting a single school system. This is affecting school systems across the country. And it's important that we share information and—so we have a better sense of the frequency of these attacks, the scope and magnitude, [00:10:00] and, really importantly, the information we need to, one, go after the bad guys, but, two, protect other school systems from those very same threats that they're facing.

Secondly, we are big, big believers in ensuring that school systems put in place a baseline of cybersecurity protections. So, this is a set of a sort of a very small number of defenses that we think every school system can and should have in place to protect themselves from the most common risks they're facing.

So, we're talking about things like implementing multifactor authentication for staff, even better if you can put it in place for students as well. We think it's critically important and know it's critically important that school systems keep their software up-to-date and install security patches when those become available from developers and to do that in a prompt way.

We know [00:11:00] it's critically important that school systems have backups of their IT systems in place so they can roll back to known good states if they're affected by malware or other sorts of issues. And it's also critically important that school systems have plans in place for how to respond to cyber incidents because we've seen when school systems don't have those plans in place, what might be considered relatively minor issues can really blow out of proportion because it can be so challenging to respond in the moment, if that is the first time that these sorts of issues have been considered.

The third thing we think is really important is that we ask more of our vendors and suppliers. So increasingly, every vendor that we work with, whether they're an edtech vendor or not, does rely on technology and its operations. And if *they're* not secure [00:12:00] in how *they* operate, it's going to be very difficult for schools to be secure. So, during procurement, during evaluation

of our vendors and suppliers, we do need to do—ask some questions about how they secure their systems and, frankly, the data and information from your school system.

Fourth, we think it is critically important that school systems seek out K-12-specific advice and guidance. There's a lot, there's no shortage of general advice and guidance for organizations of all types on how to protect themselves from cybersecurity risks, but schools operate in a unique context. We're working with minors in our—in, you know, in our student body. We are public agencies, and much of what we have to do has to be open for review, right? So—and of course we're under-resourced, particularly in the IT function, right? [00:13:00] So, there are very specific things that make us different than other sectors. And so, it's important to find that advice that speaks to your actual circumstances and school circumstances as well.

Janelle Hughes: What a fantastic list. I love what Doug outlined about sharing information regarding cyber incidents, asking questions of vendors, which is so important, and exploring existing guidance. Schools can start taking these steps now, even if they don't have the funds or resources in place to fully develop their cybersecurity posture.

I'm also seeing a few trends across our experts. What do you think Katie, if we try to compile a list of important common steps that schools can focus on first?

Katie Barnett: Yes, that sounds great, Janelle.

Janelle Hughes: Awesome. So, what I'm hearing all three experts say [00:14:00] is that it is most critical to first set up baseline protections, which include multifactor authentication, backups and emergency contact lists, as well as keeping systems and software up-to-date.

Second, complete a self-assessment or site assessment to understand the vulnerabilities unique to your school.

And finally, take advantage of existing resources to educate yourself and your school community. Each of these three steps can really go a long way toward protecting your school or school district from cyber incidents, and most can be started right away for low to no cost. What do you think about this, Katie?

Katie Barnett: It sounds great to me. And for schools and individuals that may not know where to start with accessing resources, one easy step to take right now is to check out the cybersecurity materials offered by the U.S. Department of Education and its REMS TA Center. REMS has multiple [00:15:00] resources and training opportunities to support this topic. In addition to the other podcast episodes mentioned, we also have downloadable fact sheets and training packages, as well as click-and-go Web pages that are full of cybersecurity resources.

We also have a plethora of site assessment materials so that you can begin to assess your school for cyber and other vulnerabilities.

Janelle Hughes: I wanted to touch back briefly on the COOP that Ray mentioned in his interview snippet. So, as I mentioned before, COOP stands for continuity of operations and it is essential for every school emergency operations plan to include a COOP Functional Annex, which will outline that plan for ensuring continuity of education, learning, and support activities during emergency incidents, including cyber incidents. The REMCA Center offers an online [00:16:00] course on this topic, as well as other materials.

So regardless of what step you choose to take today, any movement forward is helpful movement. And while it is true that cybersecurity and risk management are large issues, it's helpful to know that schools and school districts can take practical, positive strides towards improving school safety.

Katie Barnett: You can also follow REMS TA Center on social media, bookmark the REMS TA Center *#REMSontheAir*, and use *#REMSonthe*Air on X if you're addressing similar topics. As always, reach out to us if you want to learn more or if you have any questions related to today's topic. You can give us a call at 1-855-781-REMS, or 7367, to pose questions that we can feature on our future podcast episodes.

Also, remember that you can email us too. [00:17:00] Just reach out at info@remstacenter.org to join our mailing list. Get timely information on webinars, Web chats, and other virtual opportunities to learn and share. 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 Website and click the share tabs that appear on the screen.

Thanks again for being here with us today.

Janelle Hughes: Thank you everyone.