READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS REMS TECHNICAL ASSISTANCE CENTER

Episode 26: Cybersecurity Planning 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 back to another episode of the *#REMSontheAir* Podcast. My name is Janelle Hughes, and I'm the Project Director here at the REMS TA Center, and today I'm joined by my colleague, Amanda Everett.

Amanda Everett: Thanks, Janelle! In today's episode of *#REMSontheAir,* we will be discussing best practices in cybersecurity [00:01:00] for schools. We will provide an overview of research on this topic and discuss current efforts and best practices for preventing, responding to, and recovering from cyber threats. In this episode, we'll also hear from special guest Dr. Timothy Tillman, Chief Technology Officer for Virginia's fifth largest school district, on his experience and recommendations related to K-12 cybersecurity.

Janelle Hughes: This is such a timely episode, Amanda, and I'm really looking forward to sharing insight into how schools and school districts can strengthen their cybersecurity posture and work proactively to protect their school communities from cyber threats.

Amanda Everett: Great. Let's start with some research on the prevalence of cyberattacks on K-12 schools. First, we know that cyberattacks against schools are on the rise. The K12 Security Information Exchange's 2022 *State of K-12 Cybersecurity: Year in Review* reports that from 2016 to 2021, schools in nearly [00:02:00] every state in the country were victims of a cyberattack, with the frequency of attacks increasing from an average of about 200 a year in 2016 and 2017 to an average of about 300 a year, from 2018 to 2021.

Janelle Hughes: That's definitely concerning. And I'll add that this report also noted that past victims of reported cyberattacks included both large and small school districts with varying levels of resources allocated to cybersecurity, so we should acknowledge that a cyberattack can happen to any school at any time.

Amanda Everett: That's right, Janelle. It's also important to note that cyberattacks can be extremely damaging, resulting in a disruption in business operations, the exposure of sensitive school information, monetary loss, learning loss, the compromise of personally identifiable student and staff information (also known as PII), and damage to the school's reputation, including a loss of the community's trust [00:03:00] in the school's digital infrastructure.

Janelle Hughes: Thanks for that reminder, and it's—that this is a troubling issue facing schools, and that schools should really invest time and resources and proven strategies to strengthen their cybersecurity in order to prevent cyberattacks and prepare themselves to be able to quickly respond to and recover from a cyberattack.

Amanda Everett: Exactly. Before we jump into those strategies, let's highlight some of the Federal efforts underway to support schools in strengthening their cybersecurity posture in managing cyber threats.

Janelle Hughes: So first, the U.S. Department of Education provides resources, technical assistance, and guidance to schools on an ongoing basis for cybersecurity planning and cyber risk management through several of its offices.

The Office of Safe and Supportive Schools administers the REMS TA Center. And we provide resources and training on this topic. The Office of Educational Technology provides guidance to help schools [00:04:00] improve their understanding of the modern educational technology landscape, which is ever changing.

Also, the Student Privacy Policy Office administers the Privacy Technical Assistance Center, which provides training and technical assistance to help schools understand cyber threats and to implement data security best practices.

Amanda Everett: It's so great that the U.S. Department of Education provides so many resources to help schools prepare for cyber threats. The U.S. Department of Homeland Security also supports these efforts through its Cybersecurity and Infrastructure Security Agency, better known as CISA.

This year CISA authored a report with a series of high-impact strategies for schools to strengthen their cybersecurity. We'll include that report in the show notes.

Janelle Hughes: Additionally, this year the White House unveiled a whole-of-government plan to improve schools' cybersecurity amidst recent increases in cyberattacks.

This plan included collaborative initiatives, several [00:05:00] Federal agencies, including the publication of a new report on defensible and resilient K-12 digital infrastructure, the creation of a K-12 government coordinating council on cybersecurity, and a $200 million pilot program proposed by the Federal Communications Commission.

Amanda Everett: Wow. There is a lot going on at the Federal level to address this issue. Thanks for sharing those initiatives, Janelle. We'll be sure to include the reports referenced in this episode in the show notes.

Janelle Hughes: Thanks, Amanda. So now that we understand the issue, let's talk about high-impact strategies for preventing, responding to, and recovering from cyberattacks.

Amanda Everett: First, schools and school districts should implement training and awareness initiatives to ensure all school community members understand the most common cyber threats and the individual actions they can take to prevent and protect against them.

Janelle Hughes: That's right. So, let's pivot now and hear from Dr. Tillman about [00:06:00] his understanding of how K-12 schools are situated in the cybersecurity landscape.

Dr. Timothy Tillman (Recorded): You know, in K-12, we face the same basic threats that any other business would face—or any other government entity, for that matter. We are not unique. We are not protected. We face the exact same problems, the exact same scale, the exact same threats, and ransoms and everything else that any other organization would face. We do see, from time to time, an uptick in things like ransomware and phishing attacks. We see a lot of social engineering because we tend to have a lot of employees, and those employees often are undereducated in technology use. So, although we face the—very similar challenges as any other organization, [00:07:00] we do have a lot of employees, and that's probably one of our biggest weaknesses.

Amanda Everett: Just as Dr. Tillman stated, ransomware and phishing attacks are common cyber threats. Schools and school districts can also become victims of denial-of-service attacks, business email compromise scams, and data breaches.

Dr. Tillman also mentioned one challenge. Schools are managing the cybersecurity awareness and understanding of all staff members, which can be tough for a large school district. This is another reason why schools and school districts should manage ongoing coordinated efforts to train staff members on cybersecurity best practices.

Janelle Hughes: Exactly. We also want to acknowledge that school staff are incredibly busy, and implementing new cybersecurity controls takes time and effort. So, let's hear again from Dr. Tillman about the importance of getting buy-in from everyone within the school district. [00:08:00]

Dr. Timothy Tillman (Recorded): It has been challenging in K-12 to implement a cybersecurity program. It has been difficult to get buy-in from a large number of users who often see technology as a hindrance—or not necessarily technology, but the policies and procedures around technology—as being a hindrance to productivity. You know, a teacher in a classroom does not want to be bogged down with multifactor authentication. They want to be able to log in, get it over with, and start teaching. They don't want to be bogged down by password changes. They don't want to be bogged down by screen timeouts and all of the basic controls that we need to put in place to protect data and to protect systems.

So, implementing a program has, for me, been a challenge more in understanding people, more than understanding the technology. It's been about [00:09:00] trying to meet everyone's needs while understanding that in the background, I have a baseline of cybersecurity and controls that I need to put in place. And that I need to convince people that these are good for them and that we can—we can save time, we can save effort, we can save money, we can make things better in the long run, even though the user population is often resistant to change.

Additionally, we have had to work with our schoolboard and our administrators to really get buy-in in terms of cheerleading and in terms of getting them to really understand that everybody has this shared responsibility of not just allowing the IT department to take on all of the efforts of cybersecurity, but that everyone has a role to play. And that starts at the top. That starts with our board members, and [00:10:00] I have been lucky enough in my own district to be able to have a board that is very interested and very supportive. But, again, we are a large district, and it is often hard to get everyone on the same page. So, we are continuing to work at that. We are continuing to get buy-in to have acceptance and to not push too hard in any one direction but instead make small changes over time that hopefully are not burdensome to our user base.

Amanda Everett: Dr. Tillman had an excellent point. Cybersecurity shouldn't only be the concern of IT personnel. School districts should work collaboratively across teams to discuss the importance of cybersecurity controls for all users and to implement best practices on a long-term basis.

Janelle Hughes: It's so true. Additionally, schools and school districts should consider adding a comprehensive Cybersecurity Annex to their emergency operations plan that details the actions to [00:11:00] be taken before, during, and after a cyberattack.

Another helpful plan to have in place is an incident response plan, which focuses on how a school or school district incident response team can act quickly to respond to a cyber threat.

And we know that high-quality preparation for a cyberattack can help schools prevent one from occurring, but it can also mitigate the potential damage if an attack does occur.

Amanda Everett: Yes, another set of best practices involves continuously reviewing, practicing, and updating the Cybersecurity Annex and the incident response plan. Schools should routinely conduct exercises such as tabletop exercises that test these plans, and they should make updates to the plans based on gaps identified and lessons learned.

Janelle Hughes: And I also want to point out that not only do exercises test the effectiveness of policies and procedures for preventing, responding to, and recovering from cyber threats, but they also help key team members [00:12:00] learn their roles in carrying out those procedures.

Amanda Everett: That's right. Developing a cybersecurity training program, a comprehensive Cybersecurity Annex, an incident response plan, and a cybersecurity exercise program will provide a solid starting foundation for a strong cybersecurity posture. Let's hear again from Dr. Tillman about more best practices in cybersecurity.

Dr. Timothy Tillman (Recorded): If you read any basic framework of cybersecurity—whether it be from NIST [National Institute of Standards and Technology] or CIS [Center for Internet Security] or ISO [International Organization for Standardization] or any of the other organizations—there are basic controls that are expected to be in place for a cybersecurity program, including incident response, disaster recovery, security awareness training, multifactor authentication, basic password hygiene—all of those things are the baseline.

In my district we [00:13:00] have implemented most of those things, and they have made a big difference in our cybersecurity posture. But more importantly, it's made a difference in the expectations of our users, that they now see that we are actually acting in their best interest for some of these artifacts and some of these policies we've created. They were also involved in the creation of those policies. So, we feel like these basic controls are things that we continue to make better from year to year, but it's no longer a question of buy-in, it's no longer a question of change—it's now just what we do. And I think that's one of the most important things that a school district can move toward, is to make those broad-stroke changes quickly so that next year it's just normal practice and it's no longer a shock to the system.

Janelle Hughes: It's great to hear from Dr. Tillman about how implementing these protective measures has improved cybersecurity for [00:14:00] his school district and have helped make cybersecurity a normal part of the school culture.

I want to take a moment to underscore multifactor authentication, or MFA, as another best practice which Dr. Tillman mentioned, as well. MFA is a process whereby an individual's identity is verified by a system requiring more than a simple password before allowing access to an online account and its related data.

MFA adds an extra layer of protection, which is essentially helpful for schools and school districts that store sensitive and, most importantly, confidential student and staff information.

Amanda Everett: It's so important for schools and school districts to proactively implement these best practices before they are faced with a cyber threat.

Janelle Hughes: It is, and I also want to add that it’s a good idea for school and school district IT personnel to become familiar with the frameworks referenced by Dr. Tillman, if they aren’t already, including the National Institute of Standards and Technology [00:15:00] Cybersecurity Framework, which schools can use to guide their activities and ensure alignment of their plans and policies and resources to those best practices in cybersecurity risk management.

Amanda Everett: That’s such a good point, Janelle. It’s a great idea to align efforts with up-to-date guidance, as the technology landscape is constantly changing. Let’s hear again from Dr. Tillman about the challenges that have come up for schools, as cyber threats have evolved.

Dr. Timothy Tillman (Recorded): The primary mission of any school is to teach our kids. The tools we use in 21st century learning are computers and Chromebooks and laptops and digital curriculum and all of the Internet, right—this safe/non-safe environment—it’s safe sometimes, it’s non-safe other times. We are constantly dealing with the outside world now, whereas 20 years ago we had a walled garden. All of those digital resources are elsewhere [00:16:00] now. They’re not internal to us anymore. We have to take steps to protect ourselves and to protect the data that we trust other people with. We have to make sure that— especially our specific PII data around students is protected from people who would use it nefariously or would use it to make money or would use it to hurt our children.

That wasn’t a concern 20 years ago, 25 years ago, 30 years ago. It is a concern now. We are in a constant state of sharing data. We are in a constant state of building new databases and, you know, inputting data into other peoples’ systems. And that’s good for students. The change has been good. But we have a new responsibility now to protect the data that we generate, the data we collect and how we use it and how long we keep it [00:17:00] and all of those things. And that’s why security controls are important is because that gives us the framework under which to operate. And without it we may get caught not being prepared. And that’s really all I want to do is be prepared for what’s next.

Janelle Hughes: Dr. Tillman just shared a really important reminder. It is our responsibility to protect students’ PII. Everyone needs to keep that in mind, and that helps remind us of the importance of cybersecurity controls, especially considering the long-term damage of cyberattacks that involve data breaches.

Amanda Everett: So true, Janelle. Schools and school districts should consider implementing the best practices we’ve discussed today to ensure they are managing cybersecurity risks effectively and have policies and plans in place that address cyber threats.

Before we go, I want to add that the U.S. Department of Education and its REMS TA Center have multiple [00:18:00] resources and training opportunities to help education agencies strengthen their cybersecurity posture and prepare to prevent, respond to, and recover from cyber threats.

Our resources include a Web page, a fact sheet, an online course, a downloadable training package, a tabletop exercise, and both a virtual and live trainings by request.

Janelle Hughes: Thank you so much for tuning in today. Please remember to follow us on social media, bookmark the REMS TA Center *#REMSontheAir* hashtag, and tweet us using the *#REMSontheAIR* hashtag if you are addressing similar topics. And, as always, if you have any questions related to our discussion today, or just want to learn more, send us your questions by email or give us a call at 1-855-781-REMS, or 7367, to pose questions that can possibly be featured on the podcast.

And don't forget that you could also email us at any time at info@remstenter.org to join our mailing list, where you'll get up-to-date 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 by visiting the REMS TA Center podcast page and clicking the share tabs that appear along the left side of your screen. Thanks for tuning in today.