The Rundown podcast transcript for Performance Audit report titled ***School Districts' Self-Reported IT Security Practices and Resources*** – Released October 2021

Brad Hoff, Host and Recruiting and Training Manager: [00:00]
Welcome to The Rundown, your source for the latest news and updates from the Kansas Legislative Division of Post Audit featuring LPA staff talking about recently released reports and discussing main findings, key takeaways, and why it matters. I'm Brad Hoff. In October 2021, Legislative Post Audit released a limited-scope audit summarizing what school districts' officials self-reported related to IT security standards and resources they are using. I'm with Heidi Zimmerman, principal auditor at Legislative Post Audit, who conducted the audit. Heidi, welcome to The Rundown.

Heidi Zimmerman, Supervisor and Principal Auditor: [00:38]
Thanks for having me, Brad.

Brad Hoff, Host and Recruiting and Training Manager: [00:38]
This is an important topic because of the amount of sensitive data that school districts maintain. Talk about what types of sensitive data they do maintain and the threats they face as custodians of this data.

Heidi Zimmerman, Supervisor and Principal Auditor: [00:54]
Sure. So, school districts maintain some of the, you know, obvious things like student grades and disciplinary actions and records, but at schools also increasingly maintain medical records, mental health records, as well, sometimes it's financial information and credit card numbers from the student's parents. So, there's a lot of very important critical and confidential information that districts are now sitting on, but they face a number of threats that could result in an unauthorized person accessing that confidential information. So, for example, a phishing scam, which is when email is used to trick someone into providing access to the network to someone who should not have that access. So, in that case, that person might see information they're not really meant to see and then take that information and then even release it to others. And so, districts need to have some kind of controls in place to prevent that sort of, very confidential, very sensitive data from ending up with someone who should not have it. We also found that during the course of this audit that these sorts of incidences do in fact happen in school districts. We found a report from the K-12 Cybersecurity Resource Center that cataloged over 400 publicly reported IT security incidences in school districts in 2020 and that was an increase of

almost 20% over the previous year. So, schools are definitely a target for this sort of event.

Brad Hoff, Host and Recruiting and Training Manager: [02:34]
Now it is important to note that although school districts maintain a lot of sensitive data, school districts are not required to implement any specific IT controls. Elaborate on this and what you found to reach this conclusion,

Heidi Zimmerman, Supervisor and Principal Auditor: [02:50]
There are state and federal laws that restrict who has access to student data. So, for example, at the federal level, there's the Family Educational Rights and Privacy Act, which is also known more commonly as FERPA, and it requires written permission from a student's guardian to release information in that student's educational record. In Kansas, we have the Student Data Privacy Act, which restricts who districts and the Department of Education can release student data to. However, neither of these laws require districts to implement any specific IT control to prevent the disclosure of that information to an authorized people. There are also a few state laws that require state agencies to adopt certain IT security controls, but those laws do not apply to school districts. The Department of Education also does not require anything specific either. So, basically, we have a situation where districts have requirements to protect information, but no direction on specifically how to do that.

Brad Hoff, Host and Recruiting and Training Manager: [04:02]
This limited-scope audit's objective was to compile what school district report using for IT security standards and resources. To collect the information, you created a survey that you sent to all 286 school districts, and also the Kansas School for the Deaf and the Kansas School for the Blind. Tell me what you learned from this survey.

Heidi Zimmerman, Supervisor and Principal Auditor: [04:28]
So, right. We did use a survey to collect this information. Surveys of course are self-reported. So, this information is self-reported from the school district. We did get a pretty good response rate though. 51% of the districts responded to the survey, given that high rate, we do think these results are reasonably representative of kind of districts statewide, but again that survey was voluntary and that can introduce some self-selection bias, but what we asked about with some basic IT security controls. So, as I mentioned a minute ago, districts are not required to implement any specific controls, but there are good standards out there that represent good practices for all types of organizations and so we asked about some of those basic controls that those standards mentioned. Based on the survey, overall, what we found was that many school districts have not implemented, even those basic IT security controls. So, here's a few examples of things that we found. Standards suggest that staff should attend security awareness training when they're hired and then again annually, but we found that 58% of the districts do not require security awareness training for their staff at any time. Standards also say that confidential data should be encrypted anytime it's sent outside of the network, but 59% of the districts do not require confidential data to be encrypted when it leaves the district's network. Last, standards suggest organizations should perform vulnerability scans of their networks at least monthly and a vulnerability scan identify as security threats on

computers so that those threats can be addressed, but we found that 65% of the districts do not scan their computers for those vulnerabilities as often as standards suggest and that included 35% of districts that reported never scanning their computer networks. So, obviously it's concerning to us that there are so many districts that have not implemented even some of the basic IT security controls that are available to them.

Brad Hoff, Host and Recruiting and Training Manager: [06:49]
The report also discusses the barriers that school district officials cited in their survey responses, these barriers to improve IT security. What did they cite as the barriers and challenges to improve IT security?

Heidi Zimmerman, Supervisor and Principal Auditor: [07:08]
So, we asked districts to rate the significance of various barriers to implementing adequate IT security controls and staff issues were rated as some of the most significant issues. So, 45% of the districts reported that their ability to hire an adequate number of IT staff was a significant barrier. 56% said their ability to pay IT staff at competitive wage was a significant problem. We also heard some other things from districts. We heard from some that the lack of guidance from the state was a problem and this was echoed by the stakeholders we talked to as well and those people included, you know, officials from the Department of Education and a private company that provides IT services to school districts. We also talked to a service center that also provides IT to school districts. We just heard repeatedly that lack of knowledge about what was expected from the districts was a problem and many of them also told us that guidance from the state would be helpful.

Brad Hoff, Host and Recruiting and Training Manager: [08:16]
During this limited-scope audit you also spent some time looking at what other states require of school districts for IT security. Tell me about the states you reviewed and what you learned.

Heidi Zimmerman, Supervisor and Principal Auditor: [08:28]
Because this was a limited-scope audit, we had some time constraints and so we weren't able to do a comprehensive review of all 50 states. So, we don't know how many states, in total, require something from their school districts, but we did find a few states that require districts to implement some type of security control. So, that includes both New Hampshire and New York, which require their departments of education to establish minimum IT security standards for school districts to implement. Texas we found they don't require the department of education to set standards, but they do require the districts to adopt an IT security policy and to have a cybersecurity coordinator.

Brad Hoff, Host and Recruiting and Training Manager: [09:15]
Finally, what's the main takeaway of this audit report?

Heidi Zimmerman, Supervisor and Principal Auditor: [09:18]
Districts just increasingly maintained some very sensitive and confidential information and protecting that information is critical, but overall the districts have

not taken the necessary steps to provide that protection. And it seems that that may be because many don't know what steps they should take. So, getting that information to districts may help them take that first step and really improving the IT security in their school district.

Brad Hoff, Host and Recruiting and Training Manager: [09:48]
Heidi Zimmerman is a principal auditor at Legislative Post Audit. She completed a limited-scope audit that summarized what school districts officials self-reported related to IT security standards and resources they are using. Heidi, thanks for visiting The Rundown and going over the audit's findings with me.

Heidi Zimmerman, Supervisor and Principal Auditor: [10:05]
Thanks again, Brad.

Brad Hoff, Host and Recruiting and Training Manager: [10:06]
Thank you for listening to The Rundown. To receive newly released podcasts, subscribe to us on Spotify or Apple podcasts for more information about Legislative Post Audit and to read our audit reports, visit kslpa.org, follow us on Twitter @ksaudit or visit our Facebook page.