KANSAS LEGISLATIVE
DIVISION of
POST AUDIT

A Limited-Scope Performance Audit Presented to the Legislative Post Audit Committee

School Districts' Self-Reported IT Security Practices and Resources

October 2021

Report Number: L-21-010

Introduction

Legislative Post Audit staff suggested this limited-scope audit, which was authorized by the Legislative Post Audit Committee at its May 5, 2021 meeting.

Objectives, Scope, & Methodology

Our audit objective was to answer the following question:

1. What do school districts report regarding IT security standards and resources?

The scope of our work included surveying all 286 school districts, the Kansas School for the Deaf, and the Kansas School for the Blind.

We reviewed state and federal laws to understand any IT security standards or controls that apply to school districts. We also interviewed officials at several relevant organizations including the Kansas Department of Education (KSDE), a service provider, a private company that provides IT services to districts, and school districts. We created a survey to ask districts about the various IT security controls they have implemented and the resources they devote to IT security. We sent that survey to all 286 school districts, the Kansas School for the Deaf, and the Kansas School for the Blind. 147 districts responded for a response rate of 51%. Given the high response rate, we think the results are reasonably representative of districts statewide. However, returning the survey was voluntary, which can introduce a self-selection bias.

More specific details about the scope of our work and the methods we used are included throughout the report as appropriate.

Important Disclosures

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Overall, we believe the evidence obtained provides a reasonable basis for our findings and conclusions based on those audit objectives.

Many school districts have not implemented basic IT security controls.

School districts maintain sensitive data which makes them attractive targets for cyberattacks.

- School districts maintain a variety of sensitive data on students. This includes student grades, disciplinary actions, medical and mental health records, and financial information.

- School districts face many threats that could result in an unauthorized person accessing confidential data, including:
    - A data breach that involves disclosure of sensitive or protected data either accidentally or intentionally.
    - Phishing scams which involve using e-mail to trick a recipient into revealing sensitive information or providing access to the network.
    - Ransomware attacks which use software to prevent entry to the system or hold data hostage until the user makes a payment.
- Attacks on school districts have increased in recent years. In March 2021, the K-12 Cybersecurity Resource Center reported an 18% increase in IT security incidents in 2020. It cataloged 408 publicly disclosed incidents related to data breaches, ransomware, and phishing attacks. Further, a 2020 Government Accounting Office reported that large and affluent districts had disproportionally more reported data breaches than smaller districts.

Although school districts maintain sensitive data, Kansas districts are not required to implement any specific IT controls.

- IT security controls are the measures taken to protect a computer or computer network against unauthorized use or access. Properly implementing these controls makes it less likely that someone will gain access to confidential data.
- State and federal laws restrict who has access to student data. However, they do not require districts to implement IT security controls. The federal Family Educational Rights and Privacy Act requires written permission from a guardian (or from the student if they are an adult) to release information in the student's education record. The Kansas Student Data Privacy Act restricts who districts and KSDE can release certain student data to. Neither law requires districts to implement any specific IT security controls to prevent unauthorized access to those records.
- Although state laws require state agencies to adopt certain IT security controls, those laws do not apply to school districts.
    - K.S.A. 75-7202 establishes the Information Technology Executive Council (ITEC). ITEC sets the IT policies, procedures, and security standards for all state agencies.
    - Further, the Kansas Cybersecurity Act requires most executive

branch agencies to have an information security program and to implement standards in accordance with state laws.

- KSDE does not require districts to implement specific IT security controls. At this time, the department is not required to do so. Further, department officials told us they do not have the staff to oversee the districts in this area. When districts request guidance, they told us they refer them to the ITEC security standards.

Many school districts have not implemented several basic IT security controls.

- We sent surveys to all 286 school districts and the Kansas schools for the deaf and the blind. 147 districts responded for a response rate of 51%. We asked districts to report on the practices their district have currently implemented across several IT security control areas. Given the high response rate, we think the results are reasonably representative of districts statewide. However, returning the survey was voluntary, which can introduce a self-selection bias.

- **Figure 1** shows the percentage of districts that responded to the various questions about the security controls they have implemented. We selected several ITEC standards for the survey. Although districts are not required to follow ITEC, these standards are based on standards from the National Institute of Standards and Technology (NIST) and represent good practices for all types of organizations. As the figure shows, the majority of school districts reported lacking several basic IT security controls. For example:

    - 58% do not require security awareness training for their staff at any time. Standards suggest staff should attend security awareness training when hired and then annually.

    - 59% do not require confidential data to be encrypted when sending it outside the district's network. All confidential data should be encrypted anytime it is sent outside the district's network.

    - 65% do not scan their computer systems for vulnerabilities as often as standards suggest. This includes 35% of districts that reported never scanning their computer network. A vulnerability scan identifies security threats on computers that should be addressed (or "patched"). Standards suggest organizations scan their networks at least monthly.

    - 69% do not have an incident response plan. Without a plan, the risks are greater that an organization does not recognize and respond to a security incident quickly and effectively.

Additionally, 63% do not assess their IT security risks on at least an annual basis. Standards suggest that organizations have an incident response plan and assess their risks annually.

- To a lesser degree, survey respondents indicated a few other IT security weaknesses. For example, 28% of districts do not have antivirus software installed on all its networked computers or servers. Districts should install antivirus on all networked devices. Additionally, 47% of districts do not require any staff to use multi-factor authentication (MFA). MFA uses multiple techniques to verify that the user is authorized to access the system (e.g. a password and a fingerprint).

- Smaller school districts (500 or fewer students) lag behind large districts (more than 3,000 students) in implementing some security controls.

    - 67% of small districts reported having antivirus installed on all the district's computers. In contrast, 80% of large districts did.

    - 33% of small districts reported scanning computers at least monthly. In comparison, 55% of large districts do so.

    - 45% of small districts reported requiring some or all staff to use MFA, compared to 65% of large districts.

Districts reported that staffing issues and a lack of knowledge about what IT security controls to implement were significant barriers to improving IT security.

- We asked districts to rate the significance of various barriers to implementing adequate IT security controls. **Figure 2** shows how districts responded. As the figure shows, staff-related issues were the most significant barriers. Training, infrastructure resources, and management knowledge and support were cited as minor barriers.

    - About half of the districts reported that their ability to hire sufficient IT staff or to pay them competitively were significant barriers.

    - Over half of districts reported their ability to provide adequate infrastructure resources and to provide training to staff were minor barriers.

    - Slightly less than half of districts reported that management support or management knowledge were minor barriers.

- Districts reported other difficulties in our survey. Several reported that the lack of guidance from the state was problematic. Some noted that

they would like guidance or a set of requirements so they would know what controls to implement. A few also reported that it's difficult to get staff to implement security practices because they are viewed as inconvenient.

- We also interviewed several stakeholders including KSDE, a service center, a private company that provides IT services to districts, and four school districts. Every stakeholder reported that a lack of knowledge or training was a challenge they faced. Most of them also reported that guidance from the state would help them better implement IT security controls. However, a couple thought imposing requirements would be met with resistance.

- Despite these challenges, 80% of respondent districts thought their districts had done an acceptable (48%), good (28%), or very good (3%) job at implementing IT security controls overall.

Districts reported spending an annual average of about $18 per student on IT security in recent years.

- We asked districts to estimate their IT security expenditures in either the 2020 or 2021 school year. Due to the move to online education related to COVID-19, expenditures in 2021 may not be typical. We asked districts to report expenditure estimates for whichever year they thought was most typical for them. Due to time constraints, we could not verify all respondents' information (this is a limited-scope audit). We followed up on several outliers and eliminated them from the analysis to avoid distorting the results.

- On average, districts reported spending about $18 per student. This included expenditures for items such as staff, training, and software. In comparison, districts spent, on average, a total of about $16,200 per student. Additionally, the differences in IT spending per student across different sizes of districts was small.

- We looked for national benchmarks for IT security expenditures in school districts. We did not find any. As a result, we cannot say whether the expenditure estimates districts reported are reasonable or not.

- In 2020 and 2021, the federal government provided additional funding to school districts to offset expenditures related to COVID-19. The federal government allows districts to use that funding for IT security activities. To do so, the expenditure must be related to preventing, preparing for, or responding to COVID-19. KSDE officials told us they have informed districts about this. Further, they told us that some districts have already used some of their federal funds for this purpose.

Other findings

We identified three states that require school districts to implement specific IT security controls.

- Due to time constraints, we could not do a comprehensive search for IT security control requirements in other states. However, we did identify a few states that require school districts to implement security controls.

- New Hampshire statute requires its department of education to establish minimum standards for the security of student and employee data for all school districts. The standards the department chose are derived from the NIST cybersecurity framework. Further, the law requires districts to present a data governance plan to their local school board. That plan must include items such as an inventory of software applications, policies for data protection, and a breach response plan.

- New York statute requires its state education department to establish data security standards for school districts. The New York State Education Department has also adopted NIST standards for school districts. Those standards became effective for school districts in January 2020.

- Texas statute requires its school districts to adopt a cybersecurity policy and to determine risk and mitigation planning. Each district also must designate a cybersecurity coordinator.

Recommendations

1. The Kansas Legislature should consider directing KSDE to establish a set of minimum IT security standards for school districts in the form of either guidance or requirements.

Potential Issues for Further Consideration

We did not identify any issues for further consideration.

Agency Response

On September 9, 2021 we provided the draft audit report to the Kansas Department of Education. Its response is below. Agency officials generally agreed with the findings.

KSDE Response

Thank you for the opportunity to review the recent performance audit, *School Districts' Self-Reported IT Security Practices and Resources.* Our response is

limited to the sole recommendation in the report.

IT security is certainly an important topic, as noted in the report. The report recommends that the Kansas Legislature should consider directing KSDE to establish a set of minimum IT security standards for school districts in the form of either guidance or requirements. Establishment of standards by KSDE will naturally lead to school district reliance on Department staff for guidance in implementation, and auditing of the implementation of standards. This will lead to KSDE providing technical assistance to 286 public school districts and over 90 private school systems that the State Board of Education accredits, each with their own individual IT system and environment.

As noted on Page 3 of the report, the IT team at KSDE was established and has been staffed to only meet the data collection and management needs of the Department, rather than school districts. The level of support necessary for school districts to implement IT security standards would be a significant undertaking and is not possible with the current level of IT staffing at KSDE.

If the Kansas Legislature chooses to implement the LPA recommendation, there will need to be additional IT staff, and the Department would like to see that noted within the LPA recommendation.
Sincerely,

Randy Watson

Commissioner of Education

Appendix A – Cited References

This appendix lists the major publications we relied on for this report.

1. The State of K-12 Cybersecurity: 2020 Year in Review. (March 2021). *K-12 Cybersecurity Resource Center and K-12 Security Information Exchange.*

2. Recent K-12 Data Breaches Show that Students are Vulnerable to Harm. (September 2020). *Government Accountability Office.*