You have access to three resources:

1. CISA's *K-12 Cybersecurity Foundations: Getting Started Guide*
2. CISA's *K-12 Cybersecurity Foundations: Implementation Guide*
3. The transcript of *Michelle Krieger: Why Every School District Needs to Prepare for Data Protection*

Use these resources alongside everything you already know about my school district.

Your job is not to summarize the documents. Apply them to my district and tell me what we should do next.

Start by listing the district facts you are using, including:

- District size and number of schools
- IT and cybersecurity staffing
- Current technology environment
- Known security practices, policies and systems
- Budget or staffing constraints
- Current vendors and third-party applications
- State or local requirements
- Any upcoming projects, renewals or school-calendar deadlines

Separate confirmed facts from assumptions. Do not invent information about the district. If critical information is missing, ask no more than five focused questions before completing the assessment.

Evaluate the district against all eight objectives in CISA's Implementation Guide:

1. Protect student and staff login credentials.
2. Safeguard devices and other technology assets.
3. Perform, verify and test backups.
4. Develop and exercise a cyber incident response plan.
5. Provide cybersecurity training and awareness.
6. Identify and protect sensitive data.
7. Establish cybersecurity leadership and shared responsibilities.
8. Build a long-term cybersecurity plan using the NIST Cybersecurity Framework.

Give priority to the first four objectives from the Getting Started Guide. These should be addressed before recommending more advanced work unless an immediate risk requires a different order.

Use Michelle Krieger's interview to add practical district context, especially her advice about:

- Treating data protection as an organizational responsibility, not just an IT assignment

- Starting with an existing safety committee and developing a governance team
- Naming clear owners for data protection and cybersecurity decisions
- Avoiding the conflict created when IT must audit its own work
- Reviewing vendors and data privacy agreements
- Creating guardrails for staff and student AI use
- Collecting and retaining only the data the district actually needs
- Training every person with an account on the district's domain
- Explaining the purpose of phishing simulations before testing staff
- Exercising incident response plans
- Restoring and using backups instead of merely confirming that backup files exist
- Maintaining a business continuity plan for operating schools while systems are unavailable
- Using CISA, DHS and other outside partners for independent assessments

Return the following:

1. Current-state assessment

Rate each of the eight CISA objectives as:

- In place
- Partially in place
- Not in place
- Unknown

Explain the evidence behind each rating. Do not treat "unknown" as "not in place."

2. The five most important next steps

Identify the five actions that would reduce the most risk for this district.

For each action, provide:

- The specific task
- Why it matters here
- The person or department that should own it
- Other people who need to participate
- Estimated effort: low, medium or high
- Likely cost: no-cost, low-cost, moderate or significant
- Dependencies or likely obstacles
- The evidence that will prove it was completed

- The CISA practice supporting it

Make actual choices. Do not give me a 50-item checklist or label everything a top priority.

3. A practical 90-day plan

Organize the work into:

- First 30 days
- Days 31–60
- Days 61–90
- Work that can wait until later in the year

Account for the school calendar, limited IT staffing and the fact that daily operations still have to continue.

4. Leadership and ownership

Recommend who should be part of the district's cybersecurity and data-protection governance team.

If possible, begin with an existing safety, technology or leadership committee instead of creating another meeting immediately.

Provide:

- Recommended members
- The responsibility of each member
- Who should chair the group
- Which decisions should remain with IT
- Which decisions require the superintendent, cabinet, legal counsel, Human Resources, business office, curriculum leaders or school board

5. One action we can take this week

End with one specific action the IT director can begin this week without waiting for a new budget, new position or major purchase.

6. Superintendent briefing

Write a short, plain-language briefing the IT director can give the superintendent. It should explain:

- Where the district appears strongest
- Where the largest gaps are
- What should happen during the next 90 days
- What support or decision is needed from district leadership

Keep the complete response practical and concise. Use plain language. Explain technical terms. Distinguish CISA guidance from Michelle Krieger's field experience, and cite the relevant PDF page, document section or podcast timestamp for every major recommendation.

Do not claim the district is compliant with any law or framework. Flag legal or regulatory questions that should be reviewed with district counsel.

The final result should tell me what to do first, what can wait, who needs to own each task and how we will know the work is actually complete.