

FAMIS 15. Leadership Roundtables
Option B: Cybersecurity Leadership Round Table

Cybersecurity in K-12 is no longer just about tools—it's about governance, operational resilience, and leadership accountability. Today's discussion will focus on how we **quantify risk, move beyond compliance, respond effectively to incidents, and ensure leadership owns the outcome—not just IT.**

1. Risk Management (Board-Level Framing)

- "What are the top 3 cyber risks that keep your Superintendent awake?"
- "How are you translating cyber risk into business impact (instructional disruption, testing delays, payroll outages)?"
- "Do you maintain a formal risk register aligned to NIST CSF or CIS—and is it reviewed at cabinet/board level?"
- "Where are you accepting risk due to budget, staffing, or operational constraints?"
- "How are you prioritizing investments—based on compliance requirements or actual threat exposure?"

2. Compliance vs. Security (FERPA, State, Insurance Reality)

- Where does compliance help—and where does it create false confidence?"
- "How are you balancing FERPA, COPPA, state DPA requirements with real-world usability?"
- "What controls were 'checked' for compliance but failed during an incident?"
- "How is cyber insurance influencing your control environment (MFA, backups, logging, EDR)?"
- "Are audits driving your roadmap—or is your risk posture driving it?"

3. Incident Response (Leadership Readiness)

- What was your most significant incident—and what would you do differently at the leadership level?"
- "How quickly can your executive team make decisions during an active incident?"
- "Who owns the call to shut down systems vs. keep school running?"
- "How do you handle communications: parents, staff, board, media?"

FAMIS 15. Leadership Roundtables
Option B: Cybersecurity Leadership Round Table

- "Do you have a tested decision tree for: ransomware payment, data breach notification, school closure?"

4. Leadership Accountability (The Critical Gap)

- "Who ultimately owns cyber risk in your district—the CIO, Superintendent, or Board?"
- "How often is cybersecurity formally discussed at cabinet or board meetings?"
- "Do you report meaningful metrics (risk reduction, dwell time, incident trends) or just activity?"
- "How do you ensure accountability without creating a culture of fear?"
- "Is cybersecurity embedded in district strategic planning—or treated as a support function?"

5. Cross-District Lessons Learned

- "What's one control or process that made the biggest difference in your district?"
- "What failed that you thought was working?"
- "What would you fund immediately if budget wasn't a constraint?"
- "What's one 'hard lesson' you would warn other districts about?"
- "Where are you seeing the biggest emerging risks? (AI misuse, identity attacks, vendor compromise, student safety systems)"

6. Vendor & Third-Party Risk (Hot Topic for K-12)

- "How are you vetting vendors beyond a questionnaire?"
- "Do you continuously monitor vendors—or just review at contract time?"
- "Who owns vendor risk—IT, legal, curriculum, or procurement?"
- "How do you enforce data governance expectations with vendors?"

7. Culture & Workforce (Sustainability)

- "How do you build a culture of security without fatigue?"
- "What's working for staff engagement vs. what's ignored?"
- "How are you addressing staffing shortages in cybersecurity?"
- "Where are you relying on automation vs. people?"

Closing

- "What is ONE thing you are going to change when you get back?"
- "What is ONE thing districts consistently underestimate about cyber risk?"