**UEN 2023 Issue Brief
Cybersecurity**

**Background:** Cyber criminals and malicious threat actors continue to pose a significant threat to the instructional delivery and operations of Iowa school districts. When school districts are the target of these nefarious attacks, it is the children, families, and communities that are most impacted. While school districts have made efforts to increase cybersecurity measures, there is much more that could and needs to be done to help Iowa school districts be better prepared to protect against cyber criminals. It takes all players and entities of state and local government to coordinate efforts and services needed for protection from cyber security threats.

**LEADERSHIP & COORDINATION:** The State of Iowa should take a leadership role in engaging school districts directly to make recommendations and resources available to help address systemic issues that make cybersecurity risk management a challenge for Iowa school districts.

Such coordinated efforts should be made through various state agencies and offices (e.g., Iowa Department of Homeland Security, Iowa Department of Education, the Iowa General Assembly, the Iowa Governor’s Office, the Office of the Chief Information Officer, and the Area Education Agencies) to create a consortium that curates, vets, and establishes professional services and supports that school districts can elect to use and/or purchase for cybersecurity needs.

Technology services directors of the UEN reviewed the scope of needed services and support contracts and recommended that the following services should minimally be made available to schools, but as the world of technology is quickly changing, this list should not be limited:

* Virtual Chief Information Security Officer (vCISO),
* Cyber-liability Insurance,
* Vulnerability Scanning and Penetration Testing,
* Security Awareness Training,
* Security Information and Event Management (SIEM),
* Endpoint Detection and Response (EDR),
* Statewide Incident Reporting System, etc.

**FUNDING AND SUPPORTS:** Iowa Code limitations on the usage of funds was written long before cyber security was necessary. School districts currently expense cybersecurity costs out of a patchwork of funds, but staff costs must be borne by the general fund, meaning less is available for teachers and curriculum. School districts should be allowed to expense eligible cybersecurity systems, services, and improvements from the Management Fund, the Secure an Advanced Vision for Education (SAVE) fund, and the Physical Plant and Equipment Levy (PPEL). Professional development fund purposes could be expanded to allow staff training in minimizing cyber threats. Absent this expansion of levy flexibility, the Iowa General Assembly could consider additional supplemental state aid as a cybersecurity per pupil supplement to help school districts offset cybersecurity costs and increase Information Technology (IT) staffing to better support their cybersecurity posture.

Much like the physical security of a school district, the Iowa Governor’s Office should allocate federal dollars and/or other discretionary funding available to Iowa school districts to purchase additional cybersecurity resources and/or services.

State agencies should build capacity to provide outreach to Iowa schools to help them make decisions on professional service and support contracts and provide a template for a Security Policy Framework exclusively tailored for K-12 schools. Communication of best practices and trends, movement on federal legislation/policy, and other items related to cybersecurity would be beneficial for Iowa school districts. The aforementioned agencies and departments should help coordinate and streamline communication, points of contact, and the procedural demands of state and federal law enforcement. Iowa school districts need clear and concise guidance regarding best practices and actions in the event of cybersecurity incidents, including when law enforcement agencies should be notified.

**POLICY RECOMMENDATIONS:** The state should provide model policies, implementation checklists, provide funding for, and provide training and support to school districts to ensure districts have various cybersecurity essentials in place, including insurance, multifactor authentication, incident response plans and security awareness training. Without the provision of funding for these efforts, there are two bad outcomes; either diversion of general funds from education or inability of districts to protect staff, families, and students.

Cyber criminals pose a malicious threat to the instructional delivery and operation of school districts. When school districts are the target of nefarious attacks, students, families and communities are most impacted. The Iowa Legislature and executive branch should coordinate efforts to support school districts’ cyber security needs, to create a consortium that curates, vets and establishes professional services and supports from which school districts may elect to use or purchase for cybersecurity needs. To the maximum extent possible, the consortium should create options and preserve the local decision-making authority of school boards and districts in choosing services and supports needed for their community school. School districts should be able to expense cybersecurity systems, services, improvements, and training from the management fund, the state penny for school infrastructure (SAVE) fund and the physical plant and equipment levy, including the costs of cybersecurity staff.