EDUCATION

Safeguarding School Systems

Supporting K–12 districts against the growing threat of third-party cyber breaches

Cyberattacks on software suppliers, including Student Information Systems (SIS) and EdTech vendors, have surged in both frequency and scale, exposing student data to unprecedented risks and amplifying the operational and legal challenges faced by K–12 districts nationwide.

Recent high profile third-party cyber breaches, including the PowerSchool breach in late 2024 have highlighted the growing risks posed by these attacks, which the Cybersecurity and Infrastructure Security Agency (CISA) estimates more than once per school day.[1] In fact, cyber threats in K–12 schools are so prevalent that Cybersecurity and Infrastructure Security Agency (CISA) estimates there is more than one occurrence per school day on average.[2] More recently, in December 2024, there was a cybersecurity breach involving unauthorized access to PowerSchool SIS, the system used by over 30 percent of K–12 districts in the U.S.[3]

These third-party breaches, which target sensitive district data stored within vendor systems rather than the districts themselves, have become increasingly disruptive. The fallout from these incidents extends beyond immediate damage, posing long-term threats to student safety, privacy and the continuity of district operations. This growing trend necessitates urgent attention and proactive measures from superintendents to safeguard their schools and communities.

> ***Public K–12 schools experienced over 1,600 cyber incidents from 2016 to 2022. This is more than one incident per school day.***

[1] "The K–12 Cyber Incident Map," K12 Security Information eXchange (K12SIX), https://www.k12six.org/map

[2] "Cybersecurity for K–12 Education," Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/K12Cybersecurity

[3] "PowerSchool Notifies Applicable Attorneys General Offices Regarding Cybersecurity Incident," PowerSchool Student Information System, https://www.powerschool.com/security/sis-incident/

The Impact of Third-Party Attacks

The impact of these cyberattacks on school districts is profound and multifaceted, affecting not only the immediate functionality of educational systems but also the long-term safety of student data and trust from the community.

Key consequences include:

Widespread disruption

Breaches often paralyze essential services such as student data management, attendance tracking and communication systems, severely disrupting day-to-day operations.

Sensitive data compromised

Personally Identifiable Information (PII) and Health Identifiable Information (HII) of students and staff, including Social Security numbers and medical records, are common targets.

Ripple effects of stolen credentials

Attackers use stolen data to execute further attacks, including ransomware, grade manipulation and phishing campaigns targeting parents, staff and administrators.

Trust erosion

Breaches undermine trust in school systems and technology providers, fueling skepticism and slowing the adoption of digital tools meant to enhance education.

Long-term financial and personal risks

Identity theft from compromised student data, such as synthetic identities, can remain undetected for years, impacting individuals' credit and financial futures.

Many K–12 school districts' IT departments are underprepared to prevent and respond to cyberattacks, likely due to limited resources, insufficient training and a lack of comprehensive cybersecurity strategies. Responsibility for managing the district's cybersecurity extends beyond IT professionals and district leadership to students, parents, teachers, staff and other stakeholders who interact with district data. Additionally, cyber insurance alone does not mitigate the consequences of third-party cyber breaches. Without significant and regular improvements in their cybersecurity posture, districts will continue to face severe operational disruptions, compromised sensitive data and a loss of trust from their communities. It is imperative that school districts prioritize cybersecurity measures to protect their students, staff and the integrity of their educational systems.

> ***The impact of cyberattacks is significant, disrupting operations, compromising student data, and eroding community trust, while IT departments alone remain underprepared to handle these threats.***

What You Can Do Now to Minimize Your District's Risk

Education leaders must act decisively to minimize cyberattacks' impact and prepare for future incidents. Districts can mitigate risks and safeguard their operations and constituents by prioritizing the following key action steps:

> ***Education leaders must act decisively to minimize cyberattacks' impact and prepare for future incidents.***

Conduct Vendor Due Diligence

- Choose software providers with strong cybersecurity protocols and response incident plans.
- Specify the liability associated with cyber breaches in contracting terms.
- Engage procurement offices early when contracting with vendors.
- Require transparency and regular audits from vendors.

Enhance Incident Preparedness

- Develop and regularly test incident response plans, including clear communication protocols for stakeholders.
- Involve both IT vendors and school district IT departments in incident response testing.

Prioritize Cybersecurity

- Implement multifactor authentication (MFA), conduct regular security audits, and train students, parents and staff on cybersecurity best practices.
- Advocate for robust data protection measures, especially for minors' sensitive information.
- Understand the district's available financial resources dedicated to cybersecurity.
- Create transparent data governance structures aligned with the district's organizational chart, including defining user access to different types of data.

Engage Stakeholders

- Communicate transparently with parents and staff about breaches and recovery efforts to rebuild trust.
- Provide education on recognizing phishing attempts and securing personal accounts.
- Establish consistent engagement and reporting structures with school district IT leads and school boards on cyber incidents.

Implement Long-Term Monitoring

- Monitor for stolen data on dark web platforms and initiate proactive measures if data is not found.
- Offer identity protection services for students, parents and staff.
- Routinely review accounts and system access to ensure proper offboarding of students and staff who have left the district.

Strengthening Cybersecurity Posture

School districts must continuously improve their cybersecurity measures to maintain a safe and secure digital environment. Engaging third-party support is critical for K–12 school districts to mitigate the risks associated with third-party cyberattacks and proactively protect their data. Experts can provide tailored strategies to enhance data protection, plan for incident responses, apply advanced security measures and strengthen vendor management practices. Through this partnership, districts can safeguard their student information systems, restore trust in their providers and from their community, and maintain the continuity of their operations.

About Alvarez & Marsal (A&M) Education

A&M's Education Practice partners with school districts, state education agencies and education philanthropies to support leaders in operational and financial improvements, as well as full-scale organizational transformations. The team is made up of former educators and technical experts who bring a wealth of expertise and a proven track record of enhancing operational performance, financial health and academic success. A&M empowers educational leaders with innovative solutions and actionable insights, enabling more equitable and efficient resource allocation, prioritizing the protection of students and staff while navigating vulnerable situations, and ultimately driving student growth and positive academic outcomes.

About GroupSense

GroupSense is a digital risk protection services company that partners with large enterprises, law enforcement agencies, and state and municipal governments to deliver customer-specific intelligence that dramatically improves enterprise cybersecurity and fraud-management operations.

Unlike generic cyber-intelligence vendors, GroupSense uses a combination of automated and human reconnaissance to create finished intelligence that maps to each customer's specific digital business footprint and risk profile. This enables customers to immediately use GroupSense's intelligence to reduce organizational risk, without requiring any additional processing or management by overstretched security and fraud-prevention teams.

Contact us to learn more about our related support and suite of offerings.

KEY CONTACTS

Michael Potter
Senior Director, A&M

+1 248 974 6025
mpotter@alvarezandmarsal.com

Kurtis Minder
CEO, GroupSense

+1 847 902 3325
kurtis@groupsense.io

ABOUT ALVAREZ & MARSAL

Founded in 1983, Alvarez & Marsal is a leading global professional services firm. Renowned for its leadership, action and results, Alvarez & Marsal provides advisory, business performance improvement and turnaround management services, delivering practical solutions to address clients' unique challenges. With a world-wide network of experienced operators, world-class consultants, former regulators and industry authorities, Alvarez & Marsal helps corporates, boards, private equity firms, law firms and government agencies drive transformation, mitigate risk and unlock value at every stage of growth.

To learn more, visit: **AlvarezandMarsal.com**

Follow A&M on:

459513-46078/February 25
9550_FINAL

ALVAREZ & MARSAL
LEADERSHIP. ACTION. RESULTS.℠