Future-Proof Your K–12 IT Strategy

Key Insights to Building Secure, Interoperable Systems in K-12 IT

Today's schools can't afford disconnected systems or thinking. That's why the smartest strategies don't separate cybersecurity from system integration. They start with an SIS-led infrastructure that's built for both.

1. Design with Interoperability in Mind

• Adopt common data standards (like Ed-Fi or OneRoster) to ensure clean integration between SIS, LMS, financial systems, and other tools.

• Demand API-first systems that provide secure, structured, real-time access to key data points without risky manual workarounds.

• Inventory your system architecture regularly to identify redundancies, conflicting data sources, or manual touchpoints.

• Prioritize platforms that support modular integrations, letting you swap in best-in-class solutions without overhauling your stack.

2. Centralize Identity and Access Management (IAM)

• Use your SIS as a source of truth for role-based permissions. When systems are fragmented, it's harder to enforce least privilege access.

• Integrate single sign-on (SSO) and multi-factor authentication (MFA) across all platforms, including classroom tools.

• Establish automated deprovisioning workflows to revoke access when students or staff leave or change roles.

3. Build Data Context into Your Defense Strategy

• Enriched, connected data improves threat detection. When systems talk to each other, it's easier to detect anomalies or compromised accounts.

• Support incident response with clear system relationships. Identify which systems rely on others so you can isolate threats without shutting everything down.

• Include your data map in your business continuity plan. If your SIS or learning platform goes down, what are the ripple effects?

4. Train Users with Contextual, System-Specific Awareness

• Move from generic cybersecurity training to system-specific simulations. Focus on real-world workflows in your SIS, LMS, and email tools.

• Use your SIS to trigger risk-based training. For example, alert users accessing sensitive student info to potential phishing threats.

• Test awareness, not just attendance. Tabletop exercises and social engineering drills are more valuable than checkbox modules.

5. Plan for Recovery, Not Just Prevention

• Ensure backups are isolated, encrypted, and regularly tested, especially for mission-critical systems like your SIS or tuition platform.

• Include data interoperability in your disaster recovery plans. If one system is compromised, how quickly can the others recover data or function independently?

• Conduct regular tabletop exercises that simulate ransomware threats across systems, including scenarios during peak periods like back-to-school or admissions.

BY THE NUMBERS

36% of successful K–12 cyberattacks stem from compromised credentials.

71% of K–12 ransomware victims lose at least some of their backup repositories in the attack.

$6.6 M The median ransomware payment in K–12 in 2024.

80% of organizations that implement awareness training see a reduction in phishing susceptibility.

Three Pillars of a Secure, Integrated School IT Strategy

1

Interoperable Systems

Unified data across SIS, enrollment, billing, and more

2

Stronger Human Defenses

Reduced phishing risk through better user context and system access

3

Faster Detection + Recovery

Real-time insights + fewer silos = more informed response

FACTS makes your data more valuable and your school more resilient.
Explore more resources here.