

Bond Case Briefs

Municipal Finance Law Since 1971

S&P Cyber Brief: Third-Party Tech Adoption Is Testing Education Sector Cybersecurity

The education sector's growing adoption of cloud-based services and third-party technology is increasing both its cyberattack surface and the potential for incidents to cause broad and significant disruption. S&P Global Ratings considers this exposure to be an increasingly significant operational and credit quality risk for K-12 public schools and higher education institutions, with potential consequences including data breaches, service disruptions, and regulatory penalties.

What's Happening

Educational entities increasingly rely on third-party Software as a Service (SaaS) and educational technology (EdTech) providers for critical operations. These include disaster recovery, server backups, student information systems—that manage personal and demographic data, attendance, and grades—and learning management systems that host assignments, lectures, and enable hybrid learning. High-profile breaches at these providers such as Instructure/Canvas in 2026, PowerSchool over 2024, MOVEit in 2023, and BlackBaud in 2020 (see table 1) demonstrate how attackers can bypass internal defenses by targeting partner networks that are outside an education provider's direct control.

Our analysis of data provided by RiskRecon, a cybersecurity analytics group, shows that about 47% of the educational entities we rate experienced a third-party vendor breach between 2020 and 2026, up from 9% between 2010 and 2019. We consider that increased operational reliance on third-party vendors, and cyber criminals' targeting of those vendors, has materially increased cyber risk for educational institutions. While attacks have resulted in limited credit rating changes in the education sector to date, we increasingly consider the shifting operational landscape and escalating risks when assessing institutional resilience.

[Continue reading.](#)

[Free registration required.]

19-Oct-2026 | 09:26 EDT

Copyright © 2026 Bond Case Briefs | bondcasebriefs.com