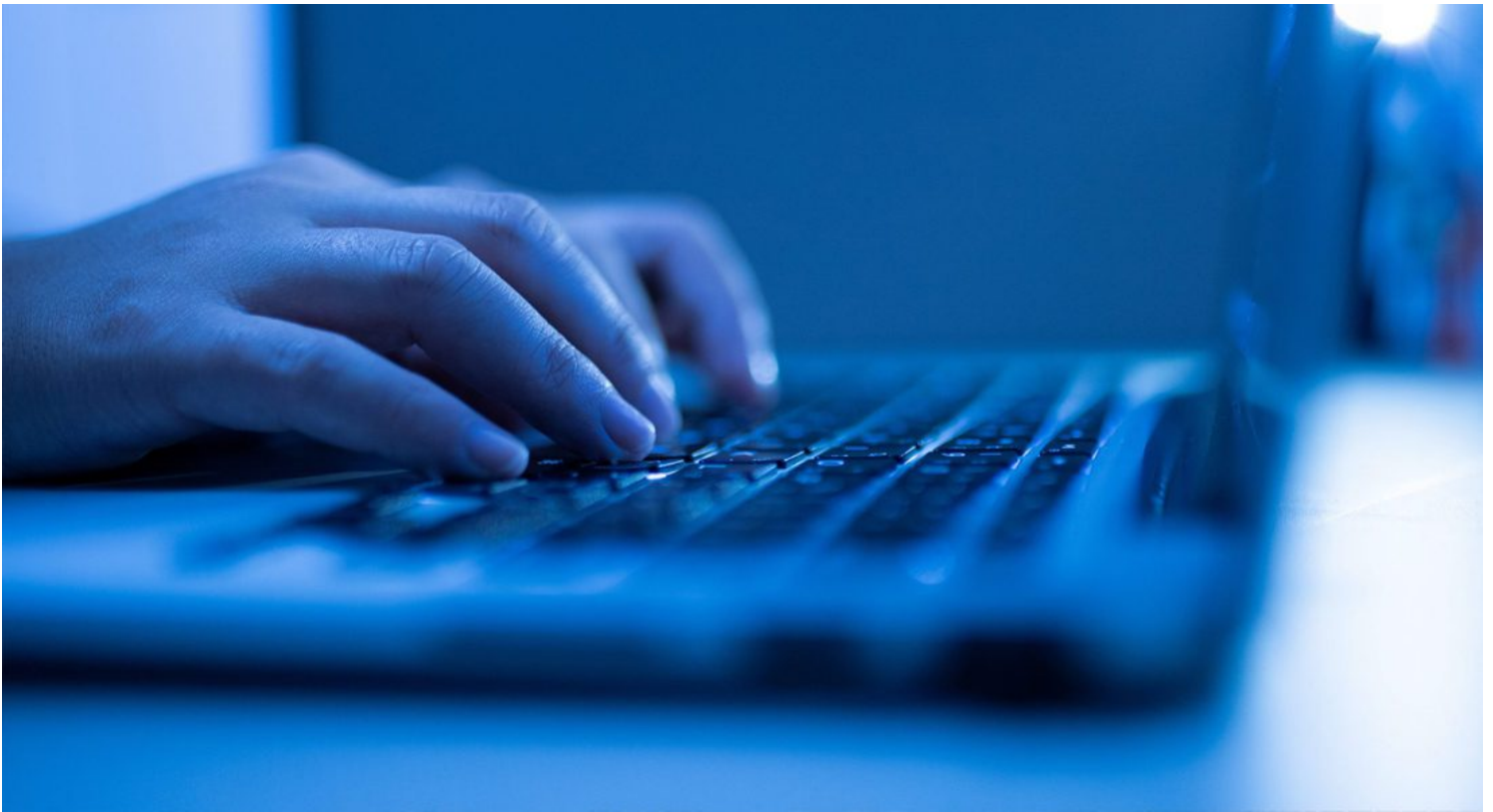


NEWS & INSIGHTS

PowerSchool breach highlights key area of vulnerability to schools

BY: [JEFFREY B. MILLER](#) | [INSIGHTS](#) | [ARTICLE](#)

JANUARY 21, 2025



On Jan. 7, the almost unthinkable happened.

PowerSchool, a third-party vendor that provides information management services to school districts, sent out a flurry of emails announcing that the company had experienced a national data breach that compromised sensitive student and faculty information.

As the incident became clearer, we learned that on or about Dec. 19, 2024, a cyber intruder gained access to PowerSchool's servers through PowerSchool's community-focused customer support portal. PowerSchool discovered

this intrusion on Dec. 28, 2024 – 10 days into the incident. The perpetrator allegedly reached out to PowerSchool, demanding money to delete the data. PowerSchool reported they paid the money contingent upon the perpetrator's promise to delete the data, and that they believe that the data was deleted. PowerSchool is now working with the FBI and other law enforcement agencies to determine what further, if anything, can be done.

While PowerSchool may have taken prompt action to address the matter, the effect on school districts, their students and staff is irreversible as the personal information of millions of students and staff has been exposed. Unfortunately, in today's digital age these kinds of data breaches are more and more common. School districts are increasingly relying on third-party vendors to manage their information to streamline their operations and enhance their efficiencies. While these third-party relationships help to ensure effective school operations, they are not without their risks – particularly when it comes to information security. Just this past year Opus, a leading provider of global compliance and risk management solutions, presented the results of its 2024 "Data Risk in the Third-Party Ecosystem" study. The study, which surveyed more than 1,000 security and risk professionals, found that a stunning **61 percent** of organizations that experienced a data breach reported the breach was caused by one of their third-party vendors.

In addition to studying organizations that had been breached, the study included an analysis of organizations that have avoided third-party data breaches. According to the study, many of these organizations had implemented one or more best practices that were strongly correlated with a reduced incidence of third-party data breaches, including:

- Establishing effective third-party management and incident response policies and procedures
- Maintaining an inventory of all third parties with whom sensitive information is shared
- Evaluating the security and privacy practices of third parties prior to contracting with them
- Solid contracting terms establishing and enforcing information privacy and security practices

Saxton & Stump is knowledgeable and experienced in helping schools address information privacy and security matters, including mitigating the threat and effect of third-party breaches. We can help you with the needed policies and procedures, to evaluate third-party cyber security practices, and to negotiate contractual provisions that protect you in the event of a breach. For help in protecting your schools, please reach out to me at (717) 566-1088 or at jbm@saxtonstump.com.

Related People

[Jeffrey B. Miller](#)

Related Services and Industries

[Information Privacy and Cybersecurity](#)