Proskauer

The PowerSchool Breach: A Privacy Lesson on Third-Party Risk Exposure

Proskauer on Privacy on **March 31, 2025**

Key Takeaways:

- Ed tech company PowerSchool's recent breach exposed the data of approximately 60 million students and 10 million educators.
- Hacker gained access via a compromised employee password and remained undetected for nine days.
- Sensitive personal data, including Social Security numbers and medical histories, was potentially compromised, raising a number of legal and regulatory concerns.
- The breach underscores the urgent need for stronger third-party oversight and security requirements.

On December 28, 2024, education technology company PowerSchool disclosed a cybersecurity breach impacting 62 million students and 9.5 million educators across the globe. The intrusion, which began on December 19, went unnoticed for nine days—providing enough time for hackers to access deeply sensitive personal information. Because of the scale of the breach and the sensitivity of the compromised data, the incident has raised serious concerns about data protection, breach notification obligations and the security oversight of third-party vendors.

What is PowerSchool?

PowerSchool serves approximately 75% of the K–12 education market and operates in more than 90 countries, including over 18,000 schools across North America. The Company is known for its Student Information System, a widely used platform that helps school districts manage K–12 student records. The system stores a broad range of personally identifiable information (PII), including student names, addresses, birthdates, and parent or guardian contact details. In many districts, it also holds more sensitive data such as Social Security numbers, medical histories, disciplinary records and individualized education plans.

The Breach

The breach purportedly stemmed from vulnerabilities with PowerSchool's customer support portal, PowerSource, due to a lack of a multifactor authentication. Exploiting this vulnerability, the intruder was able to launch an attack using an employee's compromised password, providing the intruder with unencumbered access to certain privileged functions and millions of sensitive records.

An internal investigation conducted by cybersecurity firm CrowdStrike revealed that PowerSchool only discovered the vulnerability when the attacker contacted the company directly in late December, disclosed the unauthorized access and demanded a ransom. PowerSchool leadership subsequently confirmed that the company paid the attacker, who then provided a video allegedly showing the deletion of the stolen data.

While PowerSchool reported that fewer than 25 percent of its registered students had their Social Security numbers exposed, the Company's sizable footprint suggests that figure may still potentially amount to tens of millions of affected individuals. The scale of the breach is further highlighted by PowerSchool's statewide contracts in Alabama, North Carolina, and South Carolina, along with school districts in at least 35 other states that have notified students and families. This is only compounded by the fact that at the center of the breach is children's personal data, which is especially sensitive given concerns around identity theft and the opening of fraudulent accounts.

Regulatory Implications and Legal Exposure

The breach raises a number of regulatory concerns. Under the Family Educational Rights and Privacy Act (FERPA), schools and their service providers are obligated to protect student education records[FAM1] . If any health-related information was collected or stored as part of school health programs, the incident could also fall under the scope of the Health Insurance Portability and Accountability Act (HIPAA), depending on the nature of the data and the entities involved. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2018); Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (1996). In addition to federal regulations, many states have their own data breach notification and consumer privacy laws. Statutes like the California Consumer Privacy Act (CCPA), along with similar laws in other jurisdictions, may trigger requirements for disclosure, remediation, and potential enforcement actions. Cal. Civ. Code § 1798.100 et seq. (Cal. 2024).

The Broader Issue: Third-Party Risk in the Digital Ecosystem

This breach underscores the growing challenge of managing cybersecurity risk in third-party relationships. Many organizations depend on external vendors to handle sensitive data and support core digital infrastructure, but that reliance comes with significant risk.

Organizations that work with vendors—or process sensitive data of any kind—should view this incident as a warning. Vulnerabilities in third-party system can lead to widespread consequences, including regulatory scrutiny, legal liability, loss of public trust and lasting reputational damage.

Key Lessons for Managing Third-Party Cyber Risk

- **Ongoing Vendor Oversight:** Risk assessments shouldn't stop after onboarding. Vendors handling sensitive or regulated data must be continuously evaluated as their risk profile evolves over time.
- **Contractual Safeguards:** Vendor agreements should clearly define security requirements like multi-factor authentication, encryption, and access controls. They should also include audit rights, indemnification clauses, and termination triggers for security failures.
- **Robust Incident Response Planning:** Organizations must have a coordinated breach response plan that includes legal, IT, communications and leadership teams. A clear timeline for notifications and compliance across jurisdictions is critical when third-party breaches occur.

View original.

Related Professionals

- **David Fioccola**
  Partner
- **Courtland Cuevas**
  Associate
- **Aaron M. Francis**
  Associate