When Edtech Becomes a Risk (And a Headache): Lessons Schools Can Learn from the Canvas Incident

May 27, 2026

By: Alfred Brunetti, Kerri Wright

As the school year buzzes through its hectic May-to-June blur, many schools and administrators are now dealing with the impacts from a data protection incident involving Canvas, the widely used learning management system from Instructure, an education technology company.

What Happened?

In early May 2026, public reporting and statements revealed that Canvas had suffered a targeted cyberattack that purportedly resulted in a massive outage and widespread inaccessibility. The attack is believed to have been carried out by the well-known "pay or leak" ransomware group ShinyHunters, and its timing could not have been worse for teachers and students alike. For most schools, late spring brings the crush of final exams, end-of-year projects, grading, student assessments, and closing out the academic year. A disruption to a deeply embedded learning management system during this window is not merely a technology inconvenience. It can affect instruction, communication, records, parent trust, and even advancement.

The data reportedly exposed by the incident includes names, email addresses, student ID numbers, and other personal information, such as user communications exchanged through the platform. At present, Instructure has not confirmed if passwords, dates of birth, government identifiers, or financial information were compromised, although the investigation remains ongoing.

While the exact scope of the incident remains unknown, the attackers claim to have accessed and exfiltrated data associated with hundreds of millions of users across thousands of institutions spanning elementary, secondary, and higher education. That claim of large-scale impact appears to be empirically supported by direct reports from numerous universities, including Harvard, Penn State, and Georgetown.

For schools engaging with the Canvas platform, the most pressing concerns should be determining whether information connected to their own students, staff, or institution was accessed, whether the integrity of their information remains intact, which categories of information were involved, and what obligations may now follow.

What Do We Need to Know?

Schools should resist the tempting instinct to treat an incident suffered by a vendor as just the vendor's problem – especially when that vendor manages or has access to the personal information of students and staff. Even when the technology provider is the direct target of a cyberattack, the school will still have its own homework to do. That assignment often includes, for example, evaluating legal notification duties, communicating with families, preserving records, reporting to state agencies, reviewing insurance requirements, and examining whether the vendor met its contractual obligations.

Under the federal Family Educational Rights and Privacy Act (FERPA), schools generally remain responsible for how personally identifiable information from education records is disclosed and protected. Educational technology vendors often receive student information under FERPA's "school official" exception, but that exception is not automatic. The vendor must be performing an institutional service or function for which the school would otherwise use its own employees; the vendor must be under the school's direct control with respect to the use and maintenance of education records; and the vendor's use and redisclosure of student information must be limited.

That is why the contract with the vendor itself matters. In an incident like this, a district or institution's vendor agreement is more than a simple procurement document – it's a vital starting point for evaluating the event itself and any resulting impact. It will assist your understanding of what the vendor is (or was) required to do, how quickly it must notify the school, what information it must provide, what security commitments it made, and whether any indemnification, limitation of liability, audit, insurance, or data-deletion provisions may be in play.

Regardless of whether your school is public or private, the federal Children's Online Privacy Protection Act (COPPA) may also be relevant where a digital learning platform is used by children under 13. The FTC's updated COPPA Rule strengthens obligations for covered operators, including requirements related to parental consent, separate opt-in consent for certain disclosures to third parties, and limits on retaining children's personal information for longer than reasonably necessary.

State-specific statutory obligations must also be considered, and for New Jersey schools, timing matters. New Jersey's breach notification law requires notice to affected residents "in the most expedient time possible and without unreasonable delay" when covered personal information was, or is reasonably believed to have been, accessed by an unauthorized person. In certain circumstances, the law also requires advance reporting to the Division of State Police before notifying affected individuals. Separately, an entity that maintains computerized records for another business or public entity must notify that business or public entity immediately following discovery of a breach involving covered personal information.

Schools should be careful, however, not to collapse COPPA, FERPA, state breach notification laws, and state student privacy laws into one general "student privacy" issue. They overlap, but they do not always ask the same questions. That is where schools can get tripped up - and where proper preparation may matter most.

A general vendor update may not answer the questions most important to a particular school: Was our district's data involved? Were our students affected? Did the incident involve message content or only basic account information? Are any of the affected individuals New Jersey residents? Are children under 13 involved? Did the vendor meet the contract's notice and cooperation requirements? Those questions should be answered before the district decides whether notice, parent communication, board reporting, or contract remedies are required.

What Do We Need to Do?

Schools using Canvas or any other affected edtech platform should consider taking the following steps:

1. **Confirm your institution's exposure and preserve the record.** Contact Instructure directly and request written confirmation of whether your school's data was affected. Ask for the incident timeline, the systems involved, the categories of data affected, the containment steps taken, and whether institution-specific data was accessed or exfiltrated. At the same time, preserve vendor notices, emails, screenshots, help desk tickets, internal communications, board updates, parent inquiries, technical logs, and any vendor-provided incident-related instructions. The district should be able to show what it knew, when it knew it, and what it did in response.

2. **Activate your incident response team.**
   Bring together the people who would need to make decisions if notice or parent communications become necessary.

That usually includes administration, IT, legal counsel, communications, and, where appropriate, outside cybersecurity support. Even if the breach occurred at the vendor level, the district should manage its own response.

3. **Assess legal, reporting, and notification obligations based on confirmed facts.**
   Do not assume that every cybersecurity incident triggers the same notice obligations. The analysis should account for the affected population, student residency, age and grade level, data fields involved, whether message content was accessed, whether parent or staff information was implicated, and whether there is a reasonable likelihood of misuse. New Jersey public schools should also evaluate whether the incident triggers reporting to the Division of State Police, the New Jersey Office of Homeland Security and Preparedness, or any other district-specific reporting requirement.

4. **Prepare clear parent and community communications.**
   Families do not need speculation in uncertain circumstances. They need a clear explanation of what is known, what is not yet known, what the school is doing, and what they should watch for. If the exposed information is limited to items such as names, school email addresses, student ID numbers, and platform messages, the immediate concern may be phishing, impersonation, or misuse of communications rather than traditional identity theft concerns. The response should match the actual data involved.

5. **Review the vendor agreement and use the incident as a governance checkpoint.**
   Examine the vendor agreement, data processing addendum, security schedule, service-level commitments, breach notification provision, indemnification language, and insurance obligations with legal counsel. Once the immediate response is under control, look across the rest of your edtech and administrative technology stacks. Canvas may be the headline today, but the same issues can arise with many other platforms. Schools should confirm that their major edtech vendors have appropriate breach notification timelines, security commitments, subcontractor restrictions, data-use limits, cyber insurance, and deletion obligations.

The Canvas incident is merely the latest reminder that technology contracts are not just procurement paperwork but form a key element of data protection and privacy governance. Schools can outsource the platform, but cannot outsource the responsibility for understanding what student information is involved, what the vendor promised to do, and what the school must do when something goes wrong. The districts and institutions best positioned to respond will be those that treat vendor contracts, incident response plans, and parent communications as part of their working playbooks, so they can be reviewed, pressure-tested, and updated before the next incident occurs.