Privacy Daily
Reliable news on data protection and compliance

May 15, 2026 by Kara Thompson Vol. 2, No 94

Canvas Breach Highlights Need for Proactive Cybersecurity, Response Plans, Lawyers Say

The global cyber incident that affected millions of users of the educational technology platform Canvas recently (see 2605080005) underscores the need for response planning and proactive exercises to build response protocols, privacy lawyers told us. It also highlights the risk of a single breached target impacting multiple entities downstream, they said.

The ransomware group ShinyHunters took responsibility for the breach and said the data of potentially 275 million users was compromised. Canvas parent company Instructure agreed to pay the ransom on May 11 and said that the data was returned and digital confirmation of data destruction was given.

Fisher Phillips privacy and cybersecurity lawyer Logan Booth said the “scope and scale” of the breach was its most significant characteristic. Not only is Canvas “one of the most highly used” education technology platforms in the country, it’s been around for decades, so “the longevity of the data that could be on the platform” could also pose an issue. “It’s a massive amount of information that was potentially subject to compromise,” he said in an interview.

Bond lawyer Jessica Copeland agreed. The breach of nearly 9,000 institutions signals Instructure “likely” didn’t “segregate data sufficiently to avoid lateral movement once access was gained,” she said in an email to Privacy Daily. This let the hacker steal a “significant volume” of data in a very short time period.

“Holding this much stolen data, followed by the crippling of systems during year-end/final exam crunch time made negotiating an ‘agreement’ fairly simple for this cybercriminal,” she added.

Linda Clark, a Morrison Foerster data, privacy and cyber lawyer, also noted “it was a particularly sensitive time” for disruption in access to materials typically available on Canvas, given that it was the end of the year.

It’s still uncertain what data was accessed, however, since it’s only known what the ShinyHunters hacking group claimed it stole, Booth said. Canvas, he added, should seek verification, such as through file mapping, to validate the claims.

In addition to the incident’s scope, that it “targeted … a constituency that we generally want to have enhanced protection around,” is significant as well, as there are “enhanced sensitivities around anything involving students’ information,” Booth said.

Bond’s Amber Lawyer said the education sector is “particularly unique,” since it “collects vast amounts of data, for long periods of time” and relies on “third-party vendors and technology solutions for processing, use, and storage of that data.”

Many education institutions have “shifted their data posture from on-premises solutions to cloud-based systems” from third parties, she continued, while lacking “the infrastructure and centralized resources to properly vet such solutions and to maintain adequate security measures.”

When Clark first heard about the incident, her “biggest concern” was the potential “risks to children and young adults based on the exposure of detailed information about them and how that could be used to try to extort” them.

For example, following the breach, a bad actor could send “an extortion note to a child that purports to have taken over their webcam or other connected devices” and threaten to spread “embarrassing information” about the person.

The breach is also an example of “a single supplier or a concentration risk,” Clark said. This is where a bad actor knows his actions against one entity “can impact multiple entities and move to scale.” Since Canvas was compromised, the hackers could “attempt to extort middle schools, high schools, colleges, universities, to scale” through the breach itself and “by disrupting the normal operations of those organizations.”

In the non-education context, such as financial services, the way this breach occurred “underscores that if you hit one critical vendor, you can hear the threat actor really bring pressure to bear to try to either extort or to cause other disruption,” Clark said.

The Morrison Foerster lawyer also noted the increased severity of the incident owing to its timing, at the end of the school year, when demand is high for materials often placed on the Canvas platform.

The Canvas incident impacted K-12 schools in addition to colleges and universities, so minors were part of the breach. “We as a society have ... acknowledged that [minors are] an especially vulnerable group, and yet they … could have potentially been just as implicated in a release of information or in this breach” as a college student who was over 18, Booth said.

The incident also illustrates an “important distinction” between an attack on education, which is mandatory for nearly all children, and sectors where consumers have choices about the use of their data, he said.

That an edtech platform was targeted also indicates “threat actors are no longer only going after the traditionally large, commercial for-profit enterprises,” Booth said.

Though the 2024 PowerSchool data breach of a separate student information system (see 2501220057) was “somewhat different,” Lawyer said it had a “similar impact” since K-12 schools and higher education institutes were affected globally.

She noted that PowerSchool subsequently provided credit monitoring and identity protection enrollment for victims. Thus far, Canvas hasn’t said it will do that, nor has it confirmed the “scope of information impacted ... the list of institutions impacted, or further information” about its plan for notifying affected individuals.

Clark recommended families have conversations about online safety, extortion and extortion, citing a public safety announcement from the FBI as a good resource.

Responding to a ransomware attack involves numerous questions for organizations, Booth said. There’s the “consequence of not paying the ransom,” which requires the breached entity to evaluate how “confident” it is that the threat actor actually has the data it says it does. Then the organization must think about how sensitive the information is and what the impact would be if it was leaked, he said.

On the other hand, Booth said, there’s the risk that if you pay, “are you somewhat encouraging future threat actors to undertake a similar action?”

Proof of deletion is also “hard to verify,” Copeland said, as “no one likes to trust a criminal.” Additionally, “paying can create reputational questions and may not stop later extortion attempts by the same or other threat actors.”

From a business perspective, the Canvas incident highlights “the need to proactively plan for disruptive incidents,” Clark said. Some of the universities that “did a really nice job” responding quickly “were entities that had planned for cyber incidents along with other disruptive crises.”

She recommended organizations “think through human risks [and] health and safety risks” as part of their wholistic, comprehensive plans. They should not only consider how to continue operations, but also how to support community members to “make sure they know how to get [provided] resources” and understand “the risks” of a situation.

In addition to “complying with all applicable federal, state and local laws” on handing data, Booth said education institutions should follow industry-standard cybersecurity policies. Additionally, they should stay “apprised and aware” of what those standards are and make “suitable enhancements” as necessary.

“Due diligence ... is super important,” as is “training your staff and your faculty on best practices when it comes to cybersecurity and data privacy.”

Copeland echoed both lawyers’ thoughts. Organizations need “accountable security leadership,” regular reporting on cyber risk, “disciplined data minimization and retention and a vendor-management program that treats critical service providers as part of the attack surface” from a governance standpoint. On the technical side, multifactor authentication, privileged access controls and segmentation can help too, she said.

Booth thinks it’s “very likely” that lawsuits may follow and that regulators and impacted individuals will seek recourse.

Copeland agreed. Paying the ransom “does not insulate Instructure from legal risk,” especially if state breach notification obligations apply. There could also be “questions about whether Instructure’s cybersecurity program, vendor controls, authentication safeguards, or monitoring were reasonable in light of the sensitive information they process for their customers,” she added.
As of Friday, “three purported class action lawsuits have already been filed against Instructure,” and Copeland “suspect[s]” many more will follow. “This really is just the beginning of a potentially years-long litigation journey.”

Overall, “the Canvas incident really hit home for a lot of people at a personal level, because they have children who use the platform, or college students who use the platform,” Clark said. But the breach is also “an opportunity to double down on doing proactive planning for business continuity and cyber incidents.”

Privacy Daily
Reliable news on data protection and compliance

P.O. Box 91850, Washington, DC 20090 | 1 (800) 771-9202 | privacy-daily.com | sales@warren-news.com