DATA PRIVACY & GOVERNANCE HUB

Canvas Data Breach and Ransom Agreement

MAY 20, 2026

Key Takeaways

- Canvas, a popular learning management system, was targeted in a cyberattack by a group called ShinyHunters in late April.
- The group stole 3.65 TB of data from about 9,000 educational institutions that partner with Canvas and threatened to leak it unless the company paid a ransom.
- The parent company, Instructure, said it reached an agreement with the hackers and received digital confirmation of data destruction, but experts say this cannot guarantee that the data was not copied or stored elsewhere.
- The incident has provoked renewed scrutiny over cybersecurity standards across the education sector.

What Happened

On April 29th, Instructure, the parent company of Canvas – a learning management platform used by 41% of North American educational institutions and by many others globally – detected unauthorized activity in its networks. The ShinyHunters cyber extortion group was identified in media reports as the group behind the attack. The group is reported to have stolen 3.65 TB of data from nearly 9,000 institutions.

The attackers gained access to Canvas through a vulnerability in the support ticket system within the Free-For-Teacher environment, allowing them to breach approximately 275 million records containing both academic and personal information.

Then, a second wave of unauthorized activity occurred on May 7th, during which the attackers defaced login portals at over 300 institutions. During the investigation, Canvas was temporarily taken offline, disrupting coursework and finals-week operations for millions of students and various institutions. The group threatened to leak everything stolen by May 12th. Instructure decided to negotiate with the ShinyHunters group and announced that it received the stolen data and digital confirmation of its destruction. But the company did not disclose if a ransom had been paid to the attackers.

Privacy and Governance Concerns

Even though there is no evidence that financial information or passwords were breached or compromised, the exposed data of names, emails, course details, private messages, and student IDs provides sufficient material for those who target social engineering and phishing.

Cybersecurity experts emphasize that even when digital data is returned or a digital proof of deletion is received, copies of the stolen data may re-emerge or persist.

The vulnerability exploited and the subsequent breach raised further questions about Instructure's internal monitoring, patch management, and security controls. The institutional risk exposure led school districts and universities to face operational shutdowns, communication failures, and uncertainty about whether further, stronger protective measures were needed.

Why It Matters / Policy Considerations

The breach of Canvas shows how much the education sector heavily relies on third-party digital platforms and how a single vulnerability can simultaneously disrupt thousands of institutions. A breach of this scale exposes the lack of consistent cybersecurity standards in educational technology and underscores the risks that arise when vendor oversight is inconsistent. Instructure's decision to negotiate with the attackers to meet their demands raises concerns about whether companies should pay the ransom or rely on cybercriminals to act in good faith.

This incident has triggered several class action lawsuits for negligence. These developments emphasize the need for policymakers to consider clearer breach notification requirements, sector-wide cybersecurity baselines, and possible restrictions on ransom payments. The breach demonstrates the importance of establishing stronger accountability mechanisms and creating more coordinated incident-response frameworks intended to better protect students and institutions from digital harms.