Case Study: The Cyberattack on Canvas

Kirstie Joseph

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

May 7th 2026

Introduction

The nationwide 2026 cyberattack against Canvas, which is a learning management system used by thousands of educational institutions, demonstrates how cybersecurity incidents create not only technical but also social consequences. During finals week, hackers from the cybercrime group ShinyHunters breached the platform. The hackers replaced the expected material with a ransom note that warned Instructure, the parent company of Canvas, to "pay or leak," claiming it had accessed data from millions of users, including students, teachers, and staff (Maruf et al., 2026), temporarily preventing students from accessing assignments, grades, quizzes, and coursework. The attack "stranded university students during finals week" (Maruf et al., 2026), creating widespread confusion and panic across campuses. Schools rely heavily on Canvas for communication and access to academic material, so the attack did not just affect a few users; it disrupted the educational system as a whole.

Analysis

Psychology assists in explaining the emotional impact the cyberattack had on users. Finals week is already a highly stressful, anxiety-inducing, and exhausting time for students and professors alike. Losing access to coursework during this period only worsened feelings of fear and uncertainty for students worried about meeting deadlines and grades. This stress also perpetuates the cycle of victimization because it affects decision-making, making people even more vulnerable to phishing scams and misinformation following cyber incidents. The IT Help Desk at Old Dominion University recently released an information security alert to students raising concerns about the potential for increased phishing attempts following the breach (Old Dominion University Technology Services, 2026).

Sociology explains how even one cybersecurity event can disrupt social systems within education. Universities depend on centralized digital platforms to manage communication, assignments, and exams. When Canvas was disabled, students, professors, and administrators alike experienced disruptions simultaneously. Many students feared failing classes because they could not submit assignments or access study materials. The attack also highlighted inequality because some students had backup resources while others depended entirely on Canvas.

Anthropology highlights another perspective by showing how technology has become deeply embedded in academic culture. Digital learning platforms are now viewed as essential parts of everyday education. The era of paper assignments, handwritten grading, and Scantrons serving as the primary form of examinations has largely passed. Many educators no longer provide students with tangible course materials in person, even in classes that are attended physically rather than fully online. Instead, students are often expected to independently access, download, and print materials themselves if they want physical copies. This demonstrates how society has normalized dependence on digital infrastructure.

Solutions

The Canvas attack shows the importance of combining technical cybersecurity protections with social science strategies. Although the exact vulnerability that was exploited has not been publicly disclosed by Instructure, the company released a public statement on its Security Incident Update & FAQ page. Instructure also confirmed it was “working with a best-in-class forensic firm, CrowdStrike, to support our team’s forensic analysis of this incident, as well as recommendations to further harden our environment” (Instructure, 2026). The company also stated it onboarded an additional expert vendor to conduct a comprehensive

e-discovery exercise on the compromised data in order to inform customers about the magnitude of the breach (Instructure, 2026). Universities should have additional resources rather than depending on a single platform for coursework access, similar to segmentation, so that if one system goes down, everything does not collapse, helping uphold the CIA triad principle of availability. Flexible academic policies during outages also reduce emotional stress for students affected by disruptions. The challenge in implementing these solutions would be accessibility, equity, and sourcing alternative platforms or protocols. However, a possible way to overcome these obstacles would be to take an equitable approach by providing multiple alternatives to support different circumstances.

Reflection and Conclusion

The Canvas attack proves cybersecurity is not only about protecting technology, but also about protecting people and institutions. Psychology, sociology, and anthropology help explain the impact cyberattacks have on human behavior, communication, and educational systems. A multidisciplinary approach is necessary because technical defenses alone cannot fully address the human impact of cyber threats. The incident demonstrates the growing importance of integrating social science into cybersecurity planning and response.

References

Instructure. (2026). *Security incident update & FAQs*.

https://www.instructure.com/incident_update

Maruf, R., et al. (2026, May 7). *Canvas hack strands college students during finals week*. CNN.

https://www.cnn.com/2026/05/07/us/canvas-hack-strands-college-students-finals-week

Old Dominion University Technology Services. (2026). *Nationwide security breach involving Canvas*.

https://www.odu.edu/technology-services/nationwide-security-breach-involving-canvas