TIR-20260722 Cybercrime in Higher Education: Lessons from the 2026 Canvas and PeopleSoft Incidents

7/22/2026

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

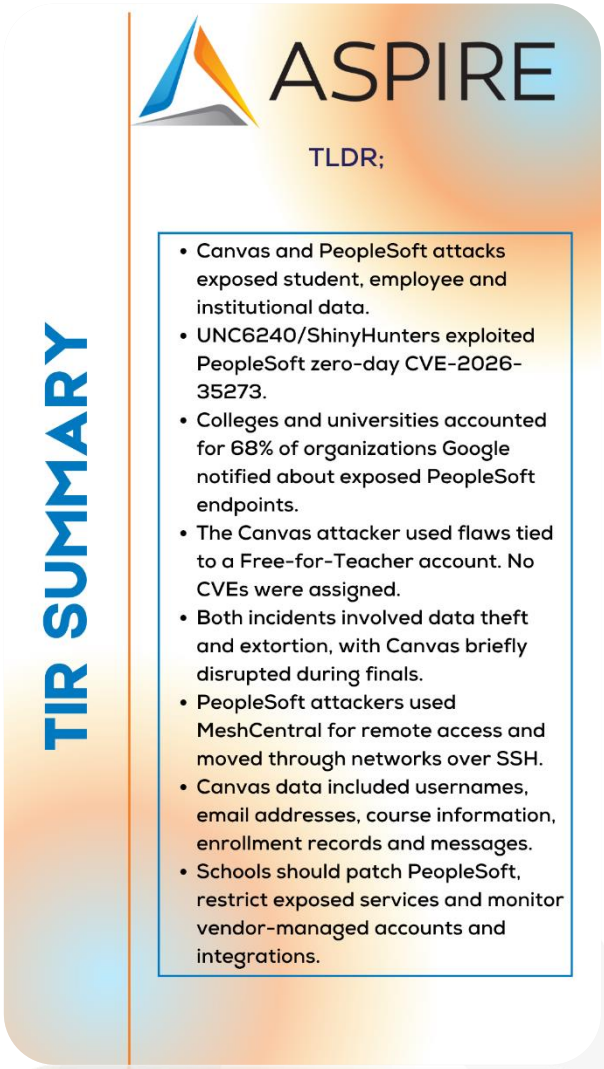
Executive Summary 3
Why Higher Education is Targeted 4
Instructure Canvas and PeopleSoft Security Incidents 5
What Threat Actors Are After 7
What We Can Learn and Recommendations 8
Conclusion 9
MITRE MAP 9
Aspire Protects 10
Indicators of Compromise (IoCs) 11
Supporting Documentation 12
Appendix II: Disclaimer 13

Executive Summary

Colleges and universities store the kind of information criminals can sell or use for fraud, including student records, payroll data and financial-aid documents. Protecting that information is difficult because thousands of students and employees need access, accounts change every semester, and individual departments often manage their own applications and older systems.

The Canvas and PeopleSoft attacks reached education organizations through different systems. In April and May 2026, an attacker used security flaws connected to Canvas Free-for-Teacher accounts to access data and briefly disrupt the platform. Between May 27 and June 9, UNC6240, also known as ShinyHunters, exploited a PeopleSoft zero-day. Google reported that colleges and universities made up [1]68% of the organizations it notified about potentially vulnerable PeopleSoft endpoints.

In each case, the attackers stole data and used it to pressure the organizations involved. The attacks also affected systems used for coursework and university administration. Schools should review which applications are exposed to the internet, who can create or use unmanaged accounts, and how outside vendors store and access institutional data.



[1] Google.com

WHY HIGHER EDUCATION IS TARGETED

Check Point ranked education as the most targeted sector in both 2025 and 2026. [2]Between January and July 2025, education organizations averaged 4,356 attacks per week, 41% more than during the same period in 2024. In June 2026, that average rose to [3]4,816 attacks per week. Government organizations ranked second at 2,836. Check Point groups schools, colleges and universities into one education category, so the figures are not limited to higher education.

A U.S. Government Accountability Office (GAO) survey found that [4]74% of Hispanic-Serving Institutions had experienced at least one cyberattack during the previous five years. The finding applies specifically to Hispanic-Serving Institutions, so it should not be used as a rate for every U.S. college.

GAO reported that colleges are targeted for personal and financial information, research data and intellectual property. Their open environments also make security harder because students, employees and visitors regularly connect to campus systems and share information online.

Threat actors frequently target higher education for several reasons:

- Universities hold valuable information - Student records, financial-aid documents, payroll files and research can be sold, used for fraud or held for extortion.
- Campus networks support a large number of users - Students, employees, visitors and outside researchers regularly connect through different devices and locations, giving attackers more opportunities to find a weak account or system.
- Accounts change throughout the year - Enrollment, graduation, temporary employment and research projects create frequent access changes that can leave old or unnecessary accounts active.

[2] CheckPoint.com
[3] CheckPoint.com
[4] Gao.gov

- Security is often spread across departments - Individual schools, laboratories or research teams may run their own applications, which can make patching and monitoring inconsistent.
- Older systems can be difficult to replace - Universities may continue using software tied to payroll, registration or financial aid because taking it offline or replacing it could interrupt campus operations.
- Colleges depend on outside providers - Learning platforms and administrative vendors store university data, and one provider breach can affect many institutions at the same time.
- Academic deadlines create pressure - An outage during finals, registration or financial-aid processing gives an extortion group more leverage because the university needs service restored quickly.

Instructure Canvas and PeopleSoft Security Incidents

Between May 27 and June 9, 2026, UNC6240, which Google associates with ShinyHunters, exploited CVE-2026-35273 in internet-facing Oracle PeopleSoft servers. The vulnerability allowed attackers to execute code remotely over HTTP without authentication. Because the activity began before Oracle disclosed the flaw and released an emergency patch on June 10, the group was using it as a zero-day.

After gaining access, the attackers installed MeshCentral agents with filenames that resembled Microsoft Azure software. They examined PeopleSoft and WebLogic configuration files, mapped other systems and tested stolen credentials against SSH services. The group compressed stolen files with zstd, and data from some victims later appeared on the ShinyHunters leak site.

Google notified more than 100 organizations whose IP addresses were associated with potentially vulnerable PeopleSoft endpoints. Most were in the United States, and colleges and universities accounted for 68%[5] of the notifications. That percentage refers

[5] Google.com

to organizations Google contacted, not confirmed victims. Google did not release a combined total of stolen records, the amount demanded or an average recovery time. Organizations responding to the campaign had to patch PeopleSoft, remove unauthorized tools and investigate activity dating to May 27.

Vulnerability Used

- CVE-2026-35273 - A critical remote code execution vulnerability in the Updates Environment Management component of PeopleTools 8.61 and 8.62.
- Attack requirements - No authentication or user interaction was required.

Instructure Canvas Security Incident

Instructure detected unauthorized Canvas activity in April 2026, and removed the attacker's access. The same threat actor returned on May 7 through a second vulnerability and changed pages shown to some students and teachers. Instructure placed Canvas in maintenance mode while it contained the activity and closed the access path. Monitoring introduced after the first intrusion detected the second attack within about 10 minutes, and the company said no additional data was taken during that event.

Both attacks involved a Free-for-Teacher account. Instructure later identified a vulnerability connected to support tickets, along with privilege-escalation paths that allowed the account to reach information beyond its intended permissions. The company fixed the affected areas and permanently discontinued Free-for-Teacher. It has not released CVE identifiers or enough technical information to reproduce either vulnerability.

The stolen information included usernames, email addresses, course names, enrollment information and messages. Instructure found no evidence that the attacker obtained passwords, dates of birth, government identification numbers, financial information, course materials or student submissions. Canvas was operating again by May 9 2026, although the outage affected schools during final examinations and grading. Instructure later reached an undisclosed agreement with the attacker, while its review of the data taken from individual institutions continued through the summer.

Vulnerabilities Used

- Free-for-Teacher support-ticket vulnerability - Used to obtain unauthorized access during the initial incident.
- Second Canvas vulnerability - Used to regain access on May 7 and alter pages presented to users.
- Privilege-escalation paths - Allowed the Free-for-Teacher account to gain access beyond its intended permissions.
- CVE status - No public CVE identifiers have been assigned.

What Threat Actors Are After

University records remain useful long after a student graduates or an employee leaves. One file may connect identity details with work history, education, relatives and financial accounts. Attackers can combine that information with data from earlier breaches to build a more complete profile of a person. The value often comes from how the records fit together rather than any one field.

- **Student and employee records** - Criminals use names, addresses, identification numbers and employment or enrollment histories for identity theft and impersonation.
- **Payroll and banking information** - Account numbers, direct-deposit details and salary records can support payment diversion and financial fraud.
- **Tax and financial-aid documents** - These files may contain Social Security numbers, income information and dependent details that can be used for fraudulent tax returns or credit applications.
- **Email addresses and account details** - Attackers use them to take over accounts, test reused credentials or identify people with access to sensitive systems.
- **Course and enrollment information** - Real class names, instructors and schedules make phishing emails more believable.

- **Private messages** - Conversations between students, faculty and staff can reveal personal circumstances that criminals may use for impersonation, fraud or extortion.
- **Research and intellectual property** - Unpublished findings, technical data and grant-funded work may be sold or used to pressure the university and its research partners.
- **System and configuration data** - Network details, API keys and application settings can help an attacker keep access, reach connected systems or prepare another intrusion.

What We Can Learn and Recommendations

The two incidents left colleges with different problems to solve. PeopleSoft was compromised through an exposed management service in software the affected organizations operated themselves.

The Canvas flaws were inside a platform managed by Instructure, leaving customers dependent on the vendor to contain the attack and determine what had been taken. Colleges need enough visibility to catch problems in their own systems, along with a plan for handling a breach at a provider they cannot investigate directly.

- **Patch and limit access to PeopleSoft** - Install Oracle's update for CVE-2026-35273, disable the Environment Management Hub where possible, and block outside access to /PSEMHUB/* and /PSIGW/HttpListeningConnector.
- **Look for earlier PeopleSoft activity** - Review logs and systems beginning May 27 because installing the patch will not remove remote-access tools, scripts or accounts left during an earlier compromise.
- **Bring unmanaged accounts under central control** - Free, guest, test and locally created accounts should follow the same MFA, approval and removal rules as other university accounts.

- **Review Canvas connections** - Check authentication and integration logs from April 25 through May 8, then rotate API keys, LTI credentials and SSO connectors that may have been exposed.
- **Limit movement from administrative servers** - Block unnecessary outbound SMB and SSH connections, and keep systems containing student or financial records separate from general campus networks.
- **Set expectations for vendors before an incident** - Contracts should address log access, security contacts, notification deadlines and the information each institution will receive after a breach.
- **Prepare for the loss of a major platform** - Document how finals, registration, payroll and financial aid will continue if a learning or administrative system is unavailable.

CONCLUSION

Colleges and universities should expect financially motivated groups to keep looking for ways into the platforms that run campus life. PeopleSoft gave UNC6240 access to administrative systems, while the Canvas breach put user information and course communications in the hands of an extortion group. The next incident could begin on campus or at a vendor, so schools need to know where their data is stored and how essential work will continue if a critical platform goes offline.

MITRE MAP

UNC6240/ShinyHunters: PeopleSoft

Initial Access	T1190 - Exploit Public Facing Application
Execution	T1059.004 – Command and Scripting Interpreter: Unix Shell
Credential Access	T1110.001 – Brute Force: Password Guessing
Discovery	T1082 – System Information Discovery T1016 – System Network Configuration Discovery

Collection	T1560.001 – Archive Collected Data: Archive via Utility
Command and Control	T1219 – Remote Access Software

SHADOW-AETHER-015/ShinyHunters: Canvas

Initial Access	T1078.004 – Valid Accounts: Cloud Accounts T1190 – Exploit Public Facing application
Privilege Escalation	T1068 – Exploitation for Privilege Escalation
Collection	T1213 – Data from Information Repositories
Impact	T1491.002 – Defacement: External Defacement

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.

  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

PeopleSoft

Network
- 142[.]11[.]200[.]186
- 142[.]11[.]200[.]187
- 142[.]11[.]200[.]188
- 142[.]11[.]200[.]189
- 142[.]11[.]200[.]190
- 176[.]120[.]22[.]24
- azurenetfiles[.]net

SHA-256
- f02a924c9ff92a8780ce812511341182c6b509d45bc59f3f7b522e37225d24fc
- d83fdb9e53c5ff03c4cb0451ea1bebd79b53f29eadc1e2fa394c7af13a86ce2f
- c7e9332731b06644fc73e0046a2a89eaa59b09f54250e9bd622467187351711f
- 68257a6f9ff196179ec03624e849927f26599eb180a7c82e14ef5bc4e93bc309
- 2ab684d93c1553fad87041b4dea97188a97e78589deee2a7bacff905564f3a35

Host and Log Artifacts
- External POST requests to /PSEMHUB/hub
- External POST requests to /PSIGW/HttpListeningConnector
- Unexpected .jsp files under the PSEMHUB.war path
- Files under PSEMHUB.war/envmetadata/transactions/
- Unexpected logs, persistent storage or scratchpad directories
- New or modified XML files under envmetadata/data/environment/

- Outbound SMB traffic on TCP 445 from PeopleSoft servers to untrusted destinations

Canvas (Behavioral)

- Canvas activity involving Free-for-Teacher accounts outside expected use
- Unusual support-ticket or privilege-change activity
- Unauthorized page changes or ransom messages
- Abnormal administrator, LTI, SSO, integration or API-key use between April 25 and May 8, 2026
- Large or unusual downloads of user, provisioning, enrollment or message data

SUPPORTING DOCUMENTATION

What this attack reveals about higher education's cybersecurity

Critical Oracle PeopleSoft Vulnerability Actively Exploited in ShinyHunters Campaign | Arctic Wolf

Top 10 Cyber Threats Facing the Education Sector in 2025

Cybersecurity in Higher Education: Don't Let the Hackers Win | EDUCAUSE Review

Strengthening Cyber Defenses in Higher Ed | Pantheon.io

How to Prevent Higher Education Cyber Attacks

Cyber Attacks Against Schools and Colleges | Arctic Wolf

ShinyHunters Targets Education Sector with Oracle PeopleSoft Exploit | Google Cloud Blog

Technology Security Alert – Ongoing Cybersecurity Incident Involving the Canvas Learning Management System (Updated May 29, 2026) | Knowledge Center

Oracle Security Alert Advisory - CVE-2026-35273

#StopRansomware: Rhysida Ransomware | CISA

#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability | CISA

Colleges hit in cyberattack by group behind Canvas breach, Google says | Higher Ed Dive

Cybersecurity for K-12 Education | CISA

Canvas Data Breach: What Students, Parents, and Faculty Need to Know - National Cybersecurity Alliance

Cyberattacks on Colleges and Universities | Fortinet

What Is the Instructure Canvas Breach? Impact, Risks, and What Institutions Should Do | Trend Micro (US)

Security Incident Update & FAQs | Instructure

Canvas owner reaches 'agreement' with threat actors after data breach | K-12 Dive

Nissan Data Breach Linked to Oracle PeopleSoft Zero-Day Hack

Active Exploitation of Oracle PeopleSoft Zero-Day (CVE-2026-35273)

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.