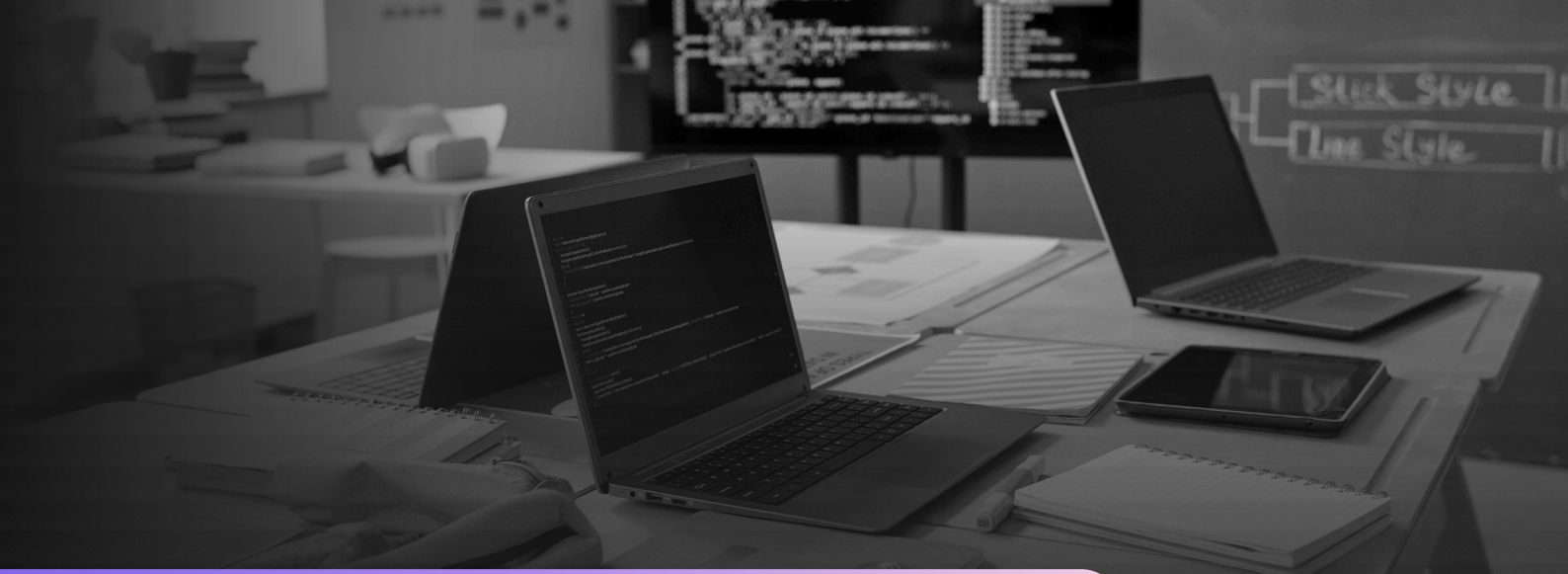
TOWERWALL WHITEPAPER

Canvas/LMS Exposure Readiness: Lessons for SaaS Security Governance

A practical guide for higher-ed leaders reviewing vendor risk, identity and integrations, and institutional readiness after the Canvas compromise.

towerwall

2026



Executive **Summary**

Recent LMS security concerns have highlighted how vendor-supplier incidents can quickly become institutional incidents. In the Canvas compromise, the reported exploit chain involved embedded JavaScript/cross-site scripting (XSS) in support tickets, execution of that script when a Canvas Support Team member viewed the ticket, exfiltration of active support-team tokens from the staff endpoint, and use of those stolen active tokens to access Canvas cloud infrastructure as a legitimate support employee and query customer databases.

Canvas responded by placing the platform in maintenance mode to investigate and implement safeguards, effectively making it unusable. The disruption derailed final exams at thousands of institutions, with hackers claiming access to data from nearly **9,000 schools.**

Based on reporting to date, the affected customer database reportedly contained names, email addresses, and similar customer information, rather than data from individual courses. While there is no indication at this time that participating institutions were directly impacted, Towerwall is helping clients to limit the risk by validating vendor notifications, LMS integrations, identity governance, testing evidence, and operational readiness.

WHY IT **MATTERS**

This was not "just a vendor problem." Even if a breach occurs outside your direct environment, the consequences (e.g., operational disruption, reputational risk, user notifications, regulatory inquiries) still fall on your institution and can have significant operational and financial impact.

This incident does not appear to be uniquely or primarily a SaaS-specific failure; rather, it reflects the chaining of several security weaknesses and the reality that institutions still bear the business impact when a core SaaS provider is compromised or unavailable.

Identity governance has become a major control point in SaaS. Enterprise SSO can strengthen identity assurance, and SCIM can improve provisioning and deprovisioning discipline, but this incident also illustrates an important nuance: even strong passwords and MFA may be bypassed once an active token is stolen. Institutions should therefore retain strong identity governance while also focusing on token handling, privileged access design, vendor monitoring, and response readiness.

WHAT WE ARE **DOING**

Proactive security mitigation involves **four areas**:

1. Understand where exposure exists through risk assessments and security reviews that map sensitive data, access, risky integrations, and vendor dependencies, supported by vulnerability management and penetration testing of SaaS-connected apps, cloud, and infrastructure.

2. Tighten identity and access governance by enforcing strong MFA, least privilege, privileged account governance, and periodic access reviews.

3. Accelerate detection and response with defined incident response plans for vendor, account, token, and integration breaches, and monitoring for unusual logins, token misuse, and suspicious cross-system activity.

4. Strengthen governance, compliance, and user awareness by assigning ownership, documenting access rules, conducting vendor reviews, requesting vulnerability assessments and penetration test results, and training users to spot phishing, protect sessions, and report suspicious activity.

Why This Matters for Business Reasons

- **Unauthorized Access of Sensitive Data:** Customer, student, faculty, and staffdata sensitivity (FERPA, GLBA, state privacy laws), depending on the systems and records involved.
- **Business Disruptions:** LMS as core academic infrastructure: disruption can impact instruction, exams, and grade integrity.
- **Third-party dependency:** Risk extends to integrations, shared identity layers (SSO), and other dependencies inside vendor ecosystems.
- **Too Much Access:** Broad platform access, over-permissioned support roles, and weak governance can multiply impact when a token or session is compromised.
- **Fines and Regulatory Oversight:** Compliance, insurance, and audit readiness: expect evidence of testing, risk assessments, and vendor oversight.
- **Impact on Reputation and Trust:** Disruptions and compromise of data can erode reputation and trust, impacting overall financial health.
- **Resilience Exposure:** Even when a breach is contained, outage, maintenance mode, or degraded service at a core SaaS provider can create immediate academic and operational consequences.

Key Questions Leadership Should Ask

Vendor Risk

- Which vendors/platforms connect to the LMS (Canvas) and what data do they access or store?
- What have we received from Canvas or related vendors regarding impact, indicators of compromise, remediation timelines, and the nature of the data exposed?
- Can the vendor provide a shared responsibility matrix, ideally including material fourth-party risks and dependencies, even if only at a high level?
- Have we asked for recent vulnerability assessments and penetration tests, and do they address the areas most relevant to this incident pattern?

Access & Identity

- Do all Canvas and SSO accounts, including admins, faculty, contractors, and service accounts, use multifactor authentication with strong factors? Are risky MFA methods disabled?
- Are admin and elevated roles reviewed regularly? Are inactive/unused accounts removed on a set cadence?
- Where do we rely on tokens, API keys, or service credentials, and how are those secrets issued, stored, rotated, monitored, and revoked?
- Do we continuously monitor for anomalous logins, token misuse, and unusual data access patterns across LMS and integrated services?
- If we use enterprise SSO and SCIM, have we confirmed where those services help—and where vendor-side sessions or active tokens may still create residual risk?

Integrations & Data Flow

- What systems connect to Canvas (APIs, LTI tools, plugins, analytics, grading tools)?
- Do any integrations rely on legacy tokens or shared credentials? Are secrets rotated and stored securely?
- What data moves into and out of Canvas? Do we have a current data map and retention policy aligned to personally identifiable information (PII), Family Educational Rights and Privacy Act (FERPA) and Gramm-Leach-Bliley Act (GLBA)?

Integrations & Data Flow

- Which vendor logs can we access directly, which are unavailable to customers, and what contractual or operational gaps does that create for investigations?

Testing & Validation

- When was our last external penetration test, and did it include LMS-related infrastructure, exposed web apps, high-risk integrations, and token-based workflows?
- Have we performed configuration reviews of the LMS, including privilege and role design?
- Do we have evidence for GLBA/FERPA audit readiness tied to LMS and integrated systems?

Incident Readiness

- Who owns vendor incident response internally (roles in IT/security, legal, communications, academic leadership)?
- Are notification and escalation paths defined (including board/leadership) and tested via tabletop exercises?
- Do we have playbooks for LMS outage/compromise scenarios, including continuity of instruction and exam integrity?
- Do our business continuity and resilience plans assume that a critical SaaS provider may be breached, degraded, or temporarily unavailable at a consequential moment?

Recommended Review Areas (Action Checklist)

- **Confirm vendor status and notifications:** Collect Canvas advisories, indicators of compromise, timelines, remediation guidance, and clarification on the types of data involved.
- **Review shared responsibility:** Ask for a documented responsibility matrix, including material fourth-party risk where possible, and record any areas where the vendor cannot provide detail.
- **Review LMS integrations:** Inventory LTI tools, API connections, tokenized access paths, and business owners; remove unused/unknown integrations.
- **Tighten SSO/MFA and privileged access:** Enforce strong MFA, least privilege,periodic role recertification, and disable unused accounts—while also reviewing token issuance, session controls, and revocation processes.
- **Validate external-facing systems:** Scan for exposed servers tied to LMS; verify secure configurations and rate limiting.
- **Monitor for anomalies:** Turn on and tune logging/alerting for suspicious logins, data exports, and token misuse; push for access to relevant vendor logs where customers do not normally receive them.
- **Prepare board summary:** Provide a concise status of impact, gaps, remediation plans, resilience posture, and need for third-party validation.

Suggested Board Talking Points

- "We are monitoring the situation with Canvas and reviewing whether our institution was affected."
- "Our review includes increased vendor diligence, validation of the vendor's reported incident details, and monitoring."
- "We are confirming whether recent assessments covered LMS-related systems, high-risk integrations, token-based access paths, and resilience planning."
- "We will update the board on any gaps, remediation steps, continuity implications, and whether independent validation is recommended."

When to Bring in a Security Services Provider

Consider third-party support (e.g., Towerwall) when:

• You need independent validation of vendor assurances, LMS configurations, and incident interpretations.

• Internal penetration testing did not cover LMS-related systems or integrations, exposed applications, identity governance, or token-related risk.

• You need help requesting or evaluating vendor vulnerability assessments, penetration test summaries, or shared responsibility documentation.

• You cannot produce evidence for GLBA/FERPA audits.

• There is suspected anomalous access, but limited detection/forensics capability across LMS.

• Vendor logging is limited or inaccessible, and you need support reconstructing impact and response options.

• You need help with rapid tabletop exercises, communications, resilience planning, or board-ready summaries.

• There is a staffing shortage, or internal teams are overloaded.

HOW TOWERWALL CAN HELP

Towerwall is offering a short **"Canvas / LMS Exposure Review"** to determine whether recent penetration testing, vendor risk, identity governance, resilience planning, and GLBA evidence are aligned with current higher-ed security expectations.

For institutions that want an independent LMS security assessment, covering integrations, privileged access, token-related risk, incident readiness, and continuity planning, Towerwall can deliver a board-ready report with **prioritized fixes**.

Appendix: 7 Questions to Ask IT/Security This Week

1. Show me the current inventory of Canvas integrations, data exchanged, and business owners.

2. List all privileged LMS roles tied to Canvas; confirm MFA, last login, last access review date, and any broad support-style access associated with each.

3. Provide evidence of recent pen test/config review that included LMS, integrations, and token-related workflows; highlight any open findings.

4. Produce the vendor communications from Canvas and a summary of our validation steps against those advisories, including what data types were reportedly exposed.

5. Provide logs/alerts for anomalous logins and data exports for the last 90 days; note any investigations.

6. Confirm the date and outcomes of the last tabletop exercise involving an LMS outage or compromise, including continuity-of-instruction decisions.

7. Share our GLBA/FERPA risk assessment sections covering LMS data flows, retention, and SaaS resilience assumptions.