cowbell

Cyber Threats Targeting the Education Sector

A global comparison of cyber risks affecting Higher Education and K-12 institutions

Executive Summary

Educational institutions are universally recognized as some of the most highly targeted organizations globally. However, Cowbell's intelligence reveals a stark divergence in who is attacking these institutions and why.

While both Higher Education (universities and colleges) and K-12 institutions (primary, secondary, and high schools) suffer from severe ransomware and social engineering attacks, their threat profiles differ significantly. Higher education is increasingly targeted by nation-state actors and hacktivists seeking intellectual property or political disruption. Conversely, K-12 schools face a massive, often overlooked risk of insider threats - frequently driven by the students themselves.

Matthieu Chan Tsin
SVP & General Manager, Cowbell Resiliency Services

The Threat Landscape: Diverging Adversaries

Both educational tiers struggle with weak cybersecurity postures due to budget constraints, relying heavily on outdated technology. However, the adversaries exploiting these weaknesses differ:

- **Higher Education (Nation-States & Hacktivism):** Universities act as massive repositories of valuable intellectual property and employ high-profile individuals in technology, foreign policy, and science. Unlike well-funded government agencies, universities lack robust cybersecurity budgets, making them lucrative targets for nation-state espionage and politically motivated Distributed Denial of Service (DDoS) attacks.
- **K-12 (Insider Threats & Data Theft):** K-12 schools manage vast amounts of student and staff personal, medical, and financial data. Alongside aggressive ransomware syndicates, K-12 faces a unique insider threat. In the UK, students caused 57% of school insider cyber incidents, often hacking networks to alter data or simply for "fun."

Notable Cyber Incidents: United States

For US brokers, this intelligence is a clear signal that K-12 school districts and universities face entirely different operational risks. K-12 districts are being targeted for their vast repositories of sensitive student data, often leading to complete operational shutdowns and severe community backlash. Meanwhile, higher education is defending against highly sophisticated, sometimes state-sponsored, adversaries. We must help our educational policyholders structure the right Cyber and management liability coverages to survive these data exposures, mitigate the actions of insider threats, and maintain the trust of their communities.

PowerSchool Data Breach (Insider Threat)

In December 2024, a major third-party breach of the PowerSchool student information system exposed the records of potentially 60 million students and teachers across North America. The US Department of Justice later identified a 19-year-old student, Matthew D. Lane, as the primary attacker. He was sentenced to four years in prison and nearly $14.1 million in restitution.

Cherokee County School District

The Interlock ransomware group caused a complete network shutdown in March 2025. The attackers stole 624 GB of data, compromising the personal information of students, parents, and staff.

Uvalde Consolidated Independent School District

A September 2025 ransomware attack disrupted critical systems, including phones, HVAC, security cameras, and student records, forcing a complete school closure for several days.

Mastery Schools (Philadelphia)

The DragonForce ransomware collective targeted this charter network, causing widespread IT outages and compromising the personal data of 37,031 students and staff.

Notable Cyber Incidents: United Kingdom

Our UK primary and secondary schools are grappling with devastating ransomware syndicates like Interlock, and our universities are increasingly being targeted by global hacktivists aiming to make geopolitical statements. For UK brokers, this highlights the necessity of moving beyond basic cyber hygiene conversations. Educational bodies need our guidance to understand that their risk profile is uniquely complex, requiring adaptive coverage to protect both safeguarding data and critical academic research.

Claud Bilbao
VP, Underwriting & Distribution UK & Australia

Anonymous Sudan DDoS Attacks (Higher Ed)

In February 2024, the hacktivist group Anonymous Sudan conducted a series of severe DDoS attacks on several prominent UK universities, including Cambridge University. The group claimed the attacks were politically motivated, citing the UK's geopolitical stances and international conflicts.

West Lothian Council (Scotland)

In May 2025, the Interlock ransomware group disrupted IT systems across more than 140 schools and nurseries. Attackers published approximately 3.3 million stolen files (2.6 terabytes of data) on the dark web.

Kido International (London)

The Radiant ransomware group compromised sensitive data, including photographs and home addresses, of approximately 8,000 children, parents, and nursery staff in September 2025.

Notable Cyber Incidents: Australia

Australian educational institutions - from state-run departments to prestigious independent colleges - are prime targets for sophisticated social engineering and data theft. The sheer volume of AI-driven phishing campaigns targeting our schools is alarming. Australian brokers play a crucial role in ensuring that these institutions have the financial resilience and expert incident response backing necessary to protect their students' futures when perimeter defenses inevitably fail.

Anthony Wall
Head of Underwriting (Australia)

Nationwide Phishing Campaign (MCTO3001)

Detected in late 2025, this large-scale campaign used AI to create "super clones" of legitimate communications, impersonating Services Australia and Centrelink. The campaign targeted schools with fraudulent emails to steal personal details, abusing reputable platforms to bypass spam filters.

Victorian Department of Education

A January 2026 breach compromised a department database through a school network, affecting over 650,000 current students across more than 1,700 government-funded schools.

Scotch College (Melbourne)

In August 2025, this prestigious independent boys' school experienced a cybersecurity breach. The school immediately shut down all servers and disabled user accounts to protect sensitive data belonging to current families and alumni.

Threat Actor Profiles

- **Nation-State Actors & Hacktivists:** Groups like Anonymous Sudan actively target higher education institutions to conduct DDoS disruptions for political leverage, while advanced persistent threats (APTs) target universities for intellectual property theft.
- **Interlock & DragonForce:** Financially motivated ransomware groups that frequently employ double-extortion techniques against K-12 districts, demanding payment for decryption keys while threatening to publish exfiltrated student data.
- **Insider Threats (Students):** A unique threat vector to K-12 education, where students leverage access to alter grades, disrupt operations, or cause massive data exposures (as seen in the PowerSchool breach).

The Sound Approach to Risk: Recommendations

- **Manage Insider & Access Risks:** Enforce strict Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC). Ensure student network privileges are heavily segmented from administrative and grading systems.
- **Establish DFIR Playbooks:** Document step-by-step incident response actions. Being prepared to respond decisively minimizes downtime and ensures compliance with strict data protection regulations regarding minors.
- **Leverage Intelligence Sharing:** Participate in collaborative organizations such as the MS-ISAC (US), K12 SIX (US), NCSC (UK), and AARNet (Australia) to access free vulnerability scanning and early warnings of sector-specific threats.

Cowbell: The Sound Approach to Risk

Cowbell delivers insurance that cuts through complexity and adapts as risks evolve. With streamlined quoting, expert guidance, and protection designed for the realities of today's threats, we make coverage easier to understand and more reliable when it matters most. Behind it all is the Hum—our constant, quiet vigilance—building stronger businesses, trusted partnerships, and the quiet confidence to keep moving forward.

cowbell®

US0064 0626