Why Academic Institutions Are Attractive Targets for Cyber Attacks

Educational institutions are in the crosshairs of sophisticated cybercriminals and nation-state actors. In Q2 2024, Microsoft ranked the education sector as the third most targeted globally, while ESET threat researchers observed intense APT (Advanced Persistent Threat) activity directed at schools and universities by China-, North Korea-, Iran-, and Russia-aligned groups.

A perfect storm of vulnerabilities makes the sector especially attractive: porous networks, large and transient user bases, limited security budgets, legacy technology, and highly valuable data. In the UK alone, 71% of secondary schools and nearly all universities reported serious security breaches over the past year, compared to only half of businesses. In the US, the K12 Security Information Exchange (K12 SIX) recorded, on average, more than one cyber-incident per school day between 2016 and 2022.

Financial gain remains the dominant motive, but espionage is a significant minority.

88%

of actor motives were financial, and 18% espionage.
Source: *Verizon: 2025 Data Breach Investigations Report, 2025.*

Without a robust cybersecurity strategy that emphasizes prevention, education providers risk not only financial and reputational damage, but also disruption to their core mission of teaching, research, and community service.

For many institutions with understaffed or overstretched IT departments, this also means embracing fully automated security solutions that can detect and respond to threats in real time — without waiting for manual intervention.

Breaches with Consequences

Cyberattacks against educational institutions are no longer isolated incidents — they carry real, tangible consequences that disrupt learning, research, and trust.

In 2023, the University of Manchester suffered a significant ransomware breach that targeted critical systems supporting healthcare-related research. The attackers exfiltrated sensitive data, prompting regulatory investigations and forcing the university to suspend several academic functions.

In the United States, the 2022 attack on the Los Angeles Unified School District — the second-largest public school system in the country — compromised data tied to more than 400,000 students and staff. The breach resulted in widespread disruption, public scrutiny, and a protracted recovery effort.

External actors are behind

62%

of the attacks in the educational services vertical,

with

59%

of those being organized crime.

Source: *Verizon: 2025 Data Breach Investigations Report, 2025.*

These cases illustrate that education is an attractive target for both criminal and state-backed threat actors due to its rich data environment and often under-resourced defenses.

Without proper cybersecurity strategy, institutions risk more than just downtime — they face erosion of public trust, legal liability, and lasting damage to academic continuity.

Key Threats Facing the Education Sector

Below are the five primary threat categories most commonly affecting educational institutions today, along with real-world examples and targeted mitigation strategies.

1. Ransomware and Phishing Attacks

Ransomware remains one of the most dominant threats in the threat landscape, frequently bringing school operations to a halt. A staff member could be tricked into clicking on a fake email claiming to be from the university IT department, prompting credential theft that later enables broader lateral access and can lead to extortion and ransom demands.

2. Insecure Personal Devices and BYOD Risks

The Bring Your Own Device (BYOD) culture in education vastly expands the attack surface. Students regularly bring personal laptops and smartphones to school and connect to the campus Wi-Fi to access learning management systems or submit assignments.

Students may unknowingly install a malicious browser extension or app that compromises their device, giving attackers a foothold inside the school network. Faculty members might connect home devices during hybrid classes, bypassing institutional controls and unintentionally spreading malware. All of this, occurring without security oversight, introduces significant vulnerabilities.

3. Cloud Application Vulnerabilities

Heavy reliance on cloud services like email, storage, and collaboration platforms has exposed schools to threats targeting these environments. Teachers and professors, as well as students, routinely use platforms like Microsoft Teams or Google Classroom to share assignments, discuss projects, and collaborate in real time.

If a compromised student account uploads a malware-laced file to a shared folder, the infection can rapidly spread. Similarly, an unmonitored administrator account with excessive privileges in a cloud dashboard could be hijacked via phishing, resulting in widespread account lockouts, data theft, and operational paralysis.

4. Data Protection and Compliance Challenges

Universities and schools manage vast amounts of sensitive personally identifiable information (PII), research data, and financial records — all of which are subject to strict regulatory oversight. Student information systems often store Social Security numbers, academic transcripts, and financial aid details.

A breach of these data may not only result in identity theft, but also trigger mandatory reporting requirements, audits, regulatory fines, and reputational fallout under laws like FERPA, GDPR, or HIPAA.

58%

of all compromised data in educational services vertical in 2024 were personal data.

Source: *Verizon: 2025 Data Breach Investigations Report, 2025.*

Additionally, universities engaged in federally funded or sensitive research — such as biotechnology, healthcare, or defense — often handle controlled unclassified information (CUI) that must meet national security compliance standards (e.g., NIST SP 800-171). A compromise here could jeopardize funding, partnerships, and institutional trust.

5. Limited IT Resources and Skills Shortages

To address these shortcomings, fully automated threat detection and response mechanisms are no longer optional. They ensure real-time threat neutralization without burdening internal IT teams, particularly in under-resourced environments.

Budgetary pressures and IT staff shortages mean that many institutions struggle to manage increasingly complex threat environments. In smaller school districts, a single IT administrator may be responsible for managing hundreds of devices, securing the

network, supporting virtual learning platforms, and implementing security policies — often without formal cybersecurity training. In higher education, understaffed security teams may lack the time or tools to continuously monitor endpoints, analyze logs, or respond rapidly to threats. This operational overload increases the chance of intrusions going undetected before damage is already done.

Tactics, Techniques, and Procedures Used Against Schools

These multi-vector attacks demand automated defenses capable of adapting in real time — far beyond what manual processes can handle. Threat actors targeting the education sector frequently deploy ransomware payloads exploiting unpatched vulnerabilities, social engineering, and spear-phishing attacks against faculty, staff, and administrators, and QR code phishing campaigns delivered via physical flyers, parking passes, and official campus communications.

Sophisticated malware designed to bypass Endpoint Detection and Response (EDR) protections has been increasingly observed, particularly in state-backed APT operations.

Attackers also often leverage compromised credentials obtained through phishing or credential stuffing to gain initial access, then move laterally across poorly segmented networks using tools like Mimikatz. Legacy software and unpatched systems present easy entry points for exploitation. In addition, ransomware groups now routinely engage in double extortion tactics, exfiltrating sensitive data before encrypting them to maximize pressure for payment.

Finally, supply chain attacks targeting educational technology vendors and service providers are an emerging concern, as upstream compromises can have cascading effects across multiple institutions. These evolving tactics underline the critical need for multilayered defenses capable of detecting and neutralizing threats at multiple stages of the attack chain.