Key Cybersecurity Challenges in the Education Sector

Digital Security
Progress. Protected.

Why Academic Institutions Are Attractive Targets?

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.

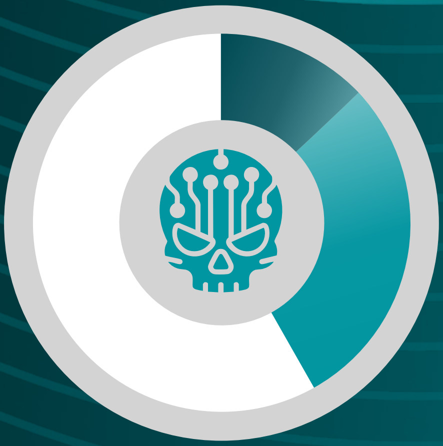
Tactics, Techniques, and Procedures Used Against Schools

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.

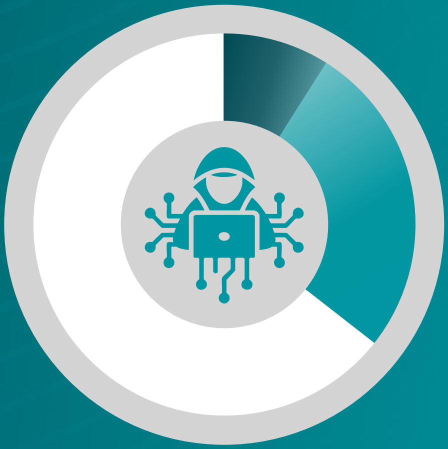


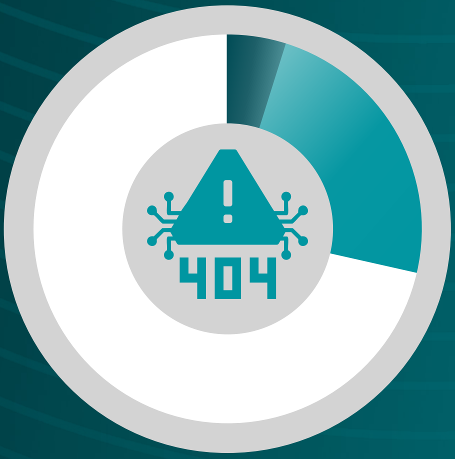
42%

of breaches were caused by malware, with ransomware responsible for **30%** of them.

36%

Hacking methods accounted for 36% of breaches, led by the use of stolen credentials at **24%**.



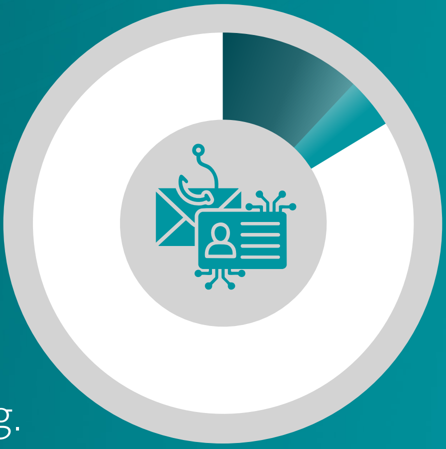


29%

Errors made up 29% of breaches, primarily due to misdelivery at **17%**.

16%

Social Engineering, one of the top three attack patterns, accounted for 16% of breaches—**77%** of those were phishing and 7% were pretexting.



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

Future Risks: An Escalating Battle

Looking ahead, educational institutions must prepare for an escalation in both sophistication and scale of cyber threats. As many experts have warned, artificial intelligence (AI) is increasingly being weaponized by adversaries, enabling hyper-personalized phishing lures and even deepfake-driven social engineering attacks targeting admissions departments, financial aid offices, and university leadership.

In 2024, IBM predicted that over 40% of security leaders expect AI-driven threats to rank among their top three organizational risks by 2026. Simultaneously, the proliferation of Internet of Things (IoT) devices on campuses is dramatically expanding the digital attack surface.

While these technologies are often deployed to enhance learning environments and campus safety, they frequently lack proper segmentation, visibility, and dedicated security controls.

Gartner's strategic technology trends for 2025 emphasize the rise of so-called ambient intelligence — systems that operate quietly in the background, blending into everyday environments. In education, this mirrors the quiet adoption of IoT without parallel investment in governance frameworks, leaving institutions vulnerable to invisible entry points.

Moreover, ongoing geopolitical tensions are expected to intensify cyber-espionage campaigns against universities, especially those involved in sensitive scientific, medical, or defense-aligned research.

Nation-state actors view higher education as a soft yet strategic target in the global cyber conflict landscape — one that blends valuable data with typically limited cybersecurity oversight. Preparing means preventing and that is undoubtedly critical these days.

40%

of security leaders expect AI threats to be a top-3 risk by 2026.

Source: Cybersecurity trends: IBM's predictions for 2024.

ESET Solutions for Scalable, Preventive Cyber Defense

Educational institutions need cybersecurity solutions that are not only powerful, but preventive, automated, and practical — adapting to budget constraints, IT staffing levels, and fast-changing threat landscapes. ESET's PROTECT Platform offers a unified, scalable ecosystem that helps schools and universities prevent, detect, and respond to threats efficiently.

The platform includes modern, fully automated Endpoint Protection with ransomware shields and remediation, and behavioral detection. ESET Cloud Office Security (ECOS) adds an essential layer of defense for Microsoft 365 and Google Workspace applications, minimizing risk from phishing, business email compromise, and malicious file sharing within collaboration tools. It also includes Anti-spoofing and Homoglyph protection, identifying threats that traditional filters or human users may overlook.

Keeping pace with best practices like patching, encryption, and policy enforcement can overwhelm limited IT teams. The ESET PROTECT Platform helps by centralizing and automating core security and IT management tasks, including Vulnerability and Patch Management (V&PM) to swiftly close known gaps.

ESET Secure Authentication delivers simple, scalable MFA, helping overcome weak password habits and preventing unauthorized access across student, staff, and admin accounts. Encryption tools assist with compliance mandates under GDPR, FERPA, and HIPAA.

For institutions with overstretched IT departments or limited in-house expertise, ESET's Managed Detection and Response (MDR) provides fully managed 24/7 protection and expert threat hunting — taking over the technical back-end so internal teams can focus on strategic and high-value tasks rather than drowning in security alerts.

MDR directly addresses the challenges of today's education threat landscape — broad attack surfaces, diverse entry points, and persistent targeted campaigns — all with the benefit of round-the-clock protection at a fraction of the cost of building internal capabilities. Whether a small district or a large research university, ESET's solutions scale intelligently and affordably, aligning with institutional size, maturity, and evolving operational needs.

SUPPORTING EDUCATION BY STRENGTHENING CYBERSECURITY

Penfield Central School District

Penfield Central School District is a K-12 public school district with approximately 5,000 students and 1,000 staff members. Located in suburban Rochester, N.Y., the district covers nearly 50 square miles, including sections of six towns: Penfield, Brighton, Perinton, Pittsford, Macedon and Walworth.

The school district, with 4,800 Windows 10 endpoints, faced significant challenges in protecting workstations from web-based threats. Their existing AV solution (from 2009) was ineffective in preventing cyber infections, resulting in considerable downtime as computers needed to be re-imaged. Additionally, the solution lacked a management console, preventing global monitoring of settings and detection of infections.

In search of stronger protection and improved management, the Penfield Central School District turned to ESET, a solution trusted for its strong reputation. In 2009, the district made a seamless transition to ESET. ESET's professional services team helped remove the old AV solution and install ESET, ensuring the clients reported back to the admin server. As an education client, the district appreciates ESET's lightweight footprint and ease of use.

KEY BENEFITS

- Seamless deployment and quick setup with central management console and policy configurations
- The solution runs quietly in the background, making it invisible to the end user
- Light footprint with minimal impact on system performance
- Reliable protection provides a secure environment with strong malware defense

> “ESET allows us to have greater uptime and reliability of our workstations, in addition to protecting the district's computer network from threats.”

Michael DiLalla
SENIOR NETWORK TECHNICIAN

Conclusion

As cyber threats against education intensify in scale and sophistication, institutions must prioritize prevention over response. Reactive security is no longer viable in an era where breaches can unfold in minutes. Automation, visibility, and zero-trust principles must be embedded into every layer of the security stack.

With the right tools and mindset — particularly prevention-first, fully automated solutions — schools and universities can shift from vulnerable to resilient, safeguarding both their mission and their most valuable digital assets.

With ESET's comprehensive, education-ready cybersecurity solutions, building that resilience becomes significantly easier and more effective.

LEARN MORE

This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network, led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

Digital Security
Progress. Protected.