Cyber Attacks on Education Sector Rise 63% Globally as Ransomware, Hacktivism and State-Backed Activity Intensify

Quorum Cyber's analysis of 425 incidents shows rising attacks with UK institutions shifting to disruption-led tactics and 91% of universities reporting breaches

EDINBURGH, UNITED KINGDOM, April 22, 2026 /EINPresswire.com/ -- Cyber attacks targeting higher and further education institutions increased by 63% year-on-year, as nation-state operations, hacktivist campaigns and organised cybercrime converge on the sector, according to new analysis from Quorum Cyber.

> "Universities are increasingly targeted both for the data they hold and the very diverse mixture of workloads and technologies."
> *Ambrose Neville, Queen Mary University of London*

The 2026 Global Cyber Risk Outlook for Higher Education shows total recorded incidents rising from 260 attacks between November 2023-October 2024 to 425 in the 12 months between November 2024-October 2025, spanning 67 countries.

The increase is underpinned by a sharp escalation across attack types. Data breaches rose by 73%, hacktivist activity by 75% and ransomware by 21%, reflecting both the growing value of academic data and the sector's expanding digital footprint.

Geopolitics and hacktivism reshaping the threat profile for universities and schools

Quorum Cyber's threat intelligence indicates that global tensions are increasingly influencing targeting patterns. Universities engaged in advanced research are facing sustained interest from nation-state actors, with Chinese-linked activity assessed as a substantial threat, particularly in areas such as AI, quantum computing and advanced materials.

Meanwhile, Iranian actors are broadening operations beyond espionage to include credential theft, ransomware and DDoS campaigns, often leveraging phishing and social engineering techniques. Hacktivism has also intensified, with attacks frequently aligned to geopolitical flashpoints. Universities have been targeted with DDoS attacks, defacements and data leaks linked to perceived positions on international conflicts, with activity assessed as "severe" heading into 2026.

Ransomware ecosystem and initial access trends

Organised cybercrime remains a persistent driver of risk and ransomware groups continue to exploit the sector's decentralised IT environments and predictable academic cycles. The ransomware group, FunkSec, accounted for 23% of observed ransomware activity, while Cl0p has issued average ransom demands exceeding $11m, highlighting the financial stakes involved.

Initial access continues to be dominated by human-layer access vectors. Phishing was responsible for 34% of ransomware incidents, while credential harvesting and infostealers remain prevalent due to high user turnover across students and staff.

The Quorum Cyber report also highlights structural challenges facing the sector. Global vulnerability disclosures exceeded 35,000 in 2025, a 21% year-on-year increase, making patch management and prioritisation increasingly complex. Combined with open research environments, hybrid learning models and legacy infrastructure, this creates a broad and difficult-to-secure attack surface.

Data shows a clear shift towards disruption-based attacks
The UK-specific data suggests a shift in attacker behaviour rather than a simple increase in volume. The insights showed that ransomware attacks remained fairly consistent but there was a fivefold increase in DDoS incidents. The sector's share of total observed attacks also increased from 2.5% to 5.15%, indicating growing targeting relative to other industries.

Jack Alexander, Senior Threat Intelligence Analyst, Quorum Cyber said: "The education sector is now dealing with a convergence of threats: nation-state actors seeking strategic advantage, hacktivists responding to geopolitical events and cybercriminal groups pursuing financial gain." He added: "What stands out in this data is how targeted and coordinated these attacks have become. In many cases, adversaries are exploiting known vulnerabilities, exposed credentials or predictable operational patterns. Universities and schools need to understand which vulnerabilities are actively being exploited, where their credentials may be exposed and how attackers are operating across the sector. The earlier these signals are identified, the greater the opportunity to disrupt attacks before they escalate into major incidents."

The findings are consistent with the UK government's Cyber Security Breaches Survey 2025, which showed the education sector is facing disproportionately high levels of cyber risk. According to their survey, 91% of higher education institutions reported experiencing a breach or attack in the last 12 months and 30% of those experienced attacks at least weekly. It also highlighted how education institutions were significantly more likely than businesses to face impersonation attacks (68% vs 34%), malware (42% vs 18%) and DDoS attacks (36% vs 5%).

Ambrose Neville, Head of Information Security, Queen Mary University of London, said: "Universities are increasingly targeted both for the data they hold and the very diverse mixture of workloads and technologies. We've observed attacks designed to interrupt teaching, research and day-to-day operations."

He continued: “The challenge for the sector is that openness and collaboration is fundamental to how higher education institutions operate. This makes it more challenging to simply lock systems away, in the way that some other industries may be able to. As a result, we prioritise security resilience. It’s critical to know where you’re exposed, spot threats early and respond quickly before incidents escalate.”

With threat activity expected to remain elevated into 2026, Quorum Cyber warns that education institutions must move beyond reactive security models and prioritise proactive threat intelligence, vulnerability prioritisation and resilience planning.

April Burghardt
Burghardt Consulting
+1 646-246-0484
april@gabdata.com
