SOPHOS

CAMPUS UNDER SIEGE: CYBER THREATS & DEFENSES IN 2025

A SOPHOS WHITEPAPER - JULY 2025

Intoduction

Higher education institutions in the U.K. form the backbone of the nation's academic and research excellence, with 260 institutions serving nearly three million students and employing over 240,000 academic staff.[1]

These organisations are not just centres of learning, but custodians of vast amounts of sensitive data, making them prime targets for cybercriminals. Unlike smaller educational bodies, universities operate complex, interconnected IT ecosystems that span research facilities, student portals, financial systems and administrative networks. This centralisation, while efficient, introduces significant cybersecurity challenges.

The threat landscape facing universities is severe. Recent government data reveals that 91% of higher education institutions experienced a cybersecurity breach in the past year, far exceeding the average for businesses (43%). Disturbingly, one in three universities reported attacks occurring at least weekly, with phishing (97%), impersonation (68%), malware (42%), and denial-of-service attacks (36%) among the most common threats.[2]

High-profile incidents, such as the Blackbaud breach[3] affecting multiple universities, the ransomware attack on a Scottish institution by the Rhysida gang,[4] and the data extortion incident at Newcastle University[5] underscore the sector's vulnerability.

[1]Higher education in numbers
[2]Cyber security breaches survey 2025: education institutions findings
[3]Blackbaud Breach Hits Nine More Universities
[4]Scottish university hit by Rhysida ransomware gang
[5]Newcastle University students' data held to ransom by cyber criminals

A treasure trove of sensitive data

The data held by higher education institutions goes far beyond names and email addresses, and includes (among other things), medical records, special educational needs assessments, criminal background checks on staff, passport details for foreign students, and project research data and intellectual property. This data is a potential goldmine for cybercriminals. Many universities don't even realise the breadth of what they store until it's too late. As one Sophos expert noted, "When you start explaining to a university that they've got medical records, criminal records, payment details and passport information on their network, they suddenly realise it's hard to keep track of and protect what's actually in their systems."

Financial incentives for attackers

While universities may not seem like traditional high-value targets, their financial resources and operational reliance on digital systems make them attractive to ransomware gangs. Disrupting research projects, student admissions, or payroll systems can force institutions into paying ransoms. The University of Manchester's 2023 cyberattack, which threatened critical systems, demonstrates how quickly operations can be paralysed. Even if a university refuses to pay, prolonged downtime, sometimes stretching for weeks, can derail academic calendars, delay research funding and incur recovery costs running into millions.

A backdoor to larger attacks

Universities and other higher education establishments are not only victims of opportunistic cybercrime, they are also seen as soft targets for state-sponsored actors. According to Microsoft's 2024 Digital Defense Report,[6] education and research institutions are now the second-most targeted sector by state-sponsored threat actors. These attackers often use educational facilities as testing grounds before moving on to higher-value targets. The interconnected nature of many universities, with shared networks across multiple sites, means that breaching one can provide access to an entire organisation.

[6] Microsoft Digital Defense Report 2024

Fragmented and overstretched IT systems

Centralised IT management across multiple sites, also introduces critical weaknesses. Many universities and colleges are made up of a patchwork of legacy systems, some decades old, alongside newer cloud-based platforms. Unsecured IoT devices, such as CCTV cameras, Raspberry Pis or design tech equipment, are frequently overlooked as potential entry points. As one Sophos security expert revealed, "We found Linux-based CCTV cameras plugged into a network that hadn't been updated or secured. Cybercriminals could easily use these as a foothold to attack the rest of the system."

The rapid shift to remote learning during COVID-19 exacerbated these risks. Most higher education providers enabled Remote Desktop Protocol and VPNs without multi-factor authentication (MFA), leaving them exposed. Today, half of all attacks analysed by Sophos Labs exploit these poorly secured remote access points.

Students and staff as the weak links

Even with robust technical defences, universities must contend with the unpredictable human element. Students, often more tech-savvy than their lecturers, can inadvertently introduce malware via personal devices. Staff clicking on phishing emails is another common form of attack.

The growing threat landscape

The digitisation of education, while transformative, has dramatically expanded the attack surface. Cloud-based learning platforms, bring-your-own-device (BYOD) policies, cashless canteens and car parks featuring QR codes at payment terminals (a tactic now exploited in "quishing" scams) create new vulnerabilities. Add to this the rise of AI-driven threats, such as deepfake voice calls (aka "vishing") mimicking trusted contacts, and it's clear that HE providers are fighting an evolving battle.

Without urgent action, the consequences extend beyond financial loss. A single breach can disrupt critical research, leak sensitive student data, and erode trust among funding bodies and international partners. As cyber threats evolve, cybersecurity must shift from an IT concern to a strategic priority for university leadership.

Ransomware in higher education

Ransomware remains a critical threat to higher education institutions, with adversaries increasingly targeting vulnerabilities in cybersecurity defences. In higher education, unknown security gaps, where universities and colleges had a weakness in their defences that they were not aware of, were the top operational root cause of an attack for 46% of respondents.[7] Though across all industries, for the third consecutive year, exploited vulnerabilities were the most common technical root cause of attacks, accounting for 32% of incidents.

Recent trends show some positive developments: data encryption rates have dropped to 50% (down from 70% in 2024), suggesting improved detection and response capabilities. However, 28% of organisations that had data encrypted also experienced exfiltration, underscoring the dual threat of encryption and theft. Smaller institutions saw lower data theft rates (22%) compared to larger ones (30%), likely due to attackers prioritising high-value targets.

While recovery times have improved, 53% of organisations fully recover within a week, the financial and human toll remains significant. The average recovery cost (excluding ransoms) dropped to over £995k, but 49% of victims still paid the ransom, the second-highest rate in six years. Additionally, IT teams face heightened stress, with 41% reporting increased anxiety and 31% experiencing staff absences due to mental health impacts.

Prolonged disruptions caused by ransomware attacks jeopardise research continuity, grant funding, and campus operations, from payroll systems to laboratory networks. Unlike lower education, where attacks primarily disrupt teaching, higher education breaches threaten intellectual property, donor databases, and global partnerships, making universities prime targets for ransomware groups seeking maximum financial leverage.

A crisis that demands immediate action

With higher education providers in the crosshairs of cybercriminals, the cost of inaction is unsustainable. With attacks growing more sophisticated, and the stakes higher than ever, the question is no longer if a trust will be targeted, but when. Universities and colleges must adopt a proactive, multi-layered security strategy to mitigate risks. While cyber insurance provides some coverage, it is not a substitute for robust defences.

Higher education providers cannot rely on piecemeal security measures. The sophisticated nature of modern cyberattacks demands an integrated, strategic approach that addresses vulnerabilities across people, processes and technology.

The first line of defence begins with closing basic security gaps that attackers routinely exploit. Unpatched systems remain one of the most common attack vectors, responsible for nearly half of all breaches, according to Sophos.

Universities need to move beyond ad-hoc patching and implement a structured vulnerability management programme that prioritises critical updates, particularly for internet-facing systems and remote access points. The risks extend beyond just computers, as seen in recent incidents, unsecured IoT devices like CCTV cameras and smart classroom equipment frequently serve as a launch pad for network-wide compromise.

[7]Sophos State of Ransomware 2025

Equally critical is the implementation of MFA across all remote access systems. MFA should extend beyond IT staff to all users accessing sensitive systems, especially those handling financial data or student welfare information.

At the device level, traditional anti-virus solutions are no longer sufficient against evolving ransomware strains. Modern endpoint protection needs to incorporate behavioural analysis, zero-day protection, anti-exploit and ransomware-blocking, and file recovery capabilities. To mitigate the rising cyber risks, increasingly cyber insurance policies are asking for proof of regular cyber training and awareness, endpoint detection and response (EDR or XDR) assuming the university or college have staff to support a 24/7 operation or a 24/7 managed detection and response (MDR) service. These advanced features can mean the difference between stopping an attack in its tracks and facing weeks of disruptive recovery efforts.

Enhancing threat visibility and response

With cybercriminals increasingly timing their attacks for evenings, weekends and holidays, higher education providers' limited IT teams struggle to maintain constant vigilance. This is where MDR services prove invaluable, providing 24/7 monitoring by security specialists who can identify and neutralise threats before they cause widespread damage. These services not only detect malicious activity, but provide education-specific threat intelligence and guaranteed response times, factors that are increasingly important for insurance compliance.

The human element remains one of the most persistent vulnerabilities. Even experienced staff can fall victim to convincing scams. Regular, realistic training simulations are essential for building staff awareness and resilience. The experience of Lancashire County Council,[8] which implemented phishing awareness programs across 500 schools, shows how such initiatives can significantly improve an organisation's human firewall.

Comprehensive network audits play a crucial role in identifying security blind spots. These should encompass not just traditional IT equipment but also legacy systems, IoT devices, and the growing array of personal devices connecting to networks. Implementing proper network segmentation can stop potential breaches, preventing an incident in one site from cascading across the entire organisation.

[8] Anti-Virus and Threat Protection Service (Sophos Central)

Preparing for the inevitable

Despite best efforts, security incidents have become a matter of when, not if. Universities need operational plans that extend far beyond theoretical documentation. Traditional incident response plans can fail when they're needed most, as they're typically stored on network drives that become inaccessible during an attack. Critical response materials, including emergency contacts, system recovery procedures and communication protocols, should be maintained in both printed and securely accessible digital formats.

The importance of reliable backups cannot be overstated in an era when most attackers specifically target backup systems. Higher education providers should implement a multi-layered backup strategy that includes regular testing of restore procedures, immutable backup storage that can't be altered by attackers and geographically dispersed copies. Monthly recovery drills help ensure that backups will actually work when needed most.

Regular simulation exercises serve as stress tests for an organisation's incident response capabilities. These tabletop scenarios reveal weaknesses in decision-making processes, communication chains and recovery timelines that might not be apparent until a real crisis occurs. They also help staff at all levels understand their roles during an incident, reducing panic and confusion when an actual attack occurs.

Leveraging external resources and collaboration

Universities and colleges don't need to face these challenges alone. The U.K.'s National Cyber Security Centre offers tailored guidance for educational institutions, covering everything from secure remote learning setups to ransomware-specific protections. While their Cyber Essentials certification shouldn't be viewed as a complete security solution, it provides a valuable baseline framework and may help reduce insurance premiums while demonstrating due diligence to regulators.

There's also significant value in collaborative defence approaches. Higher education providers can pool resources to access shared security services, participate in sector-specific threat intelligence sharing initiatives, and engage with the Department for Education cybersecurity programmes. This collective approach not only improves individual security postures but also strengthens protections across the entire education sector.

By adopting a comprehensive strategy, universities and colleges can transform their cybersecurity from a reactive cost centre to a strategic enabler of educational continuity. The goal isn't just to prevent attacks, but to build resilient organisations capable of maintaining operations even in the face of determined adversaries. Robust cybersecurity isn't just about protecting data, it's about safeguarding the learning experience itself.

SOPHOS

For more information about the Sophos Protected Classroom and how we work with schools to secure their environments 24/7/365, visit

sophos online

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: **sales@sophos.com**

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: **sales@sophos.com.au**

North America Sales
Toll Free: 1-866-866-2802
Email: **nasales@sophos.com**

Asia Sales
Tel: +65 62244168
Email: **salesasia@sophos.com**

2025-07-28-WP (MP)