EDUCATION UNDER ATTACK: CYBERSECURITY IN MATs

A SOPHOS WHITEPAPER - JULY 2025

Intoduction

Multi-Academy Trusts (MATs) represent a significant shift in the U.K.'s education landscape, with over half of state-school pupils attending academies. Unlike traditional local authority-controlled schools, MATs operate as independent entities, pooling resources across multiple schools to achieve economies of scale. This centralised approach allows for greater financial efficiency, shared IT infrastructure and streamlined administrative processes. However, it also introduces unique cybersecurity challenges.

With sensitive data, structural flaws, and a central role in education, MATs are a magnet for cyberattacks. Cyber attacks on schools have become commonplace, with attacks in West Lothian[1] and Teeside[2] occurring as recently as May 2025.

[1] West Lothian schools hit by ransomware cyberattack
[2] Middlesbrough school targeted in cyber security attack as parents warned about data breach

A treasure trove of sensitive data

MATs are custodians of vast amounts of highly sensitive information, far beyond just student grades. From medical records and special educational needs assessments to criminal background checks on staff and passport details for minibus drivers, the data held by trusts is a potential goldmine for cybercriminals. Many schools 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 school that they've got medical records, criminal records, payment details and passport information on their network, they suddenly realise they have little understanding what's actually in their systems or how it's protected."

Financial incentives for attackers

often in the millions. Ransomware gangs know that disrupting operations, whether SATs scheduling, or payroll or reporting systems, can force trusts into paying hefty ransoms.

The Harris Federation attack in 2021,[3] which cost £750,000 to recover from, demonstrates how crippling these incidents can be. Even if a trust refuses to pay, the downtime alone, sometimes stretching over a month, can have severe financial and operational repercussions.

A backdoor to larger attacks

MATs are not just victims of opportunistic cybercrime, they are also seen as soft targets for nation-state actors. According to Microsoft's 2024 Digital Defense Report,[4] education and research institutions are now the second-most targeted sector by state-sponsored hackers. These attackers often use schools as testing grounds before moving on to higher-value government or infrastructure targets. The interconnected nature of MATs, with shared networks across multiple schools, means that breaching one academy can provide access to an entire trust or even local government systems linked to them.

[3] 'They wanted $4m': Lessons for M&S from other cyber attacks
[4] Microsoft Digital Defense Report 2024

Fragmented and overstretched IT systems

The very structure that makes MATs efficient — centralised management across multiple schools — also introduces critical weaknesses. Many trusts inherit a patchwork of legacy IT 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 beachhead. As one Sophos security expert revealed, "We found Linux-based CCTV cameras plugged into a school's 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. Many MATs 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, MATs must contend with the unpredictable human element. Students, often more tech-savvy than their teachers, can inadvertently introduce malware via personal devices.

Staff clicking on phishing emails is another common form of attack. As one Sophos employee notes: "Show me a kid who wouldn't take £50 off someone to plug a USB stick into a school computer."

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, and cashless canteens create new vulnerabilities. Add to this the rise of AI-driven threats, such as deepfake voice calls (aka "vishing") mimicking headteachers, and it's clear that MATs are fighting an evolving battle.

Without urgent action, the consequences extend far beyond financial loss. A single breach can disrupt exams, leak sensitive student data and erode parental trust, potentially impacting enrolment and funding. As the education sector becomes increasingly digital, cybersecurity must move from an afterthought to a core priority for every MAT.

The impact of cyber attacks on MATs

Cyber attacks on MATs deliver severe financial, operational and reputational consequences. Recent data from Sophos paints a stark picture of an education sector under siege, with MATs bearing the brunt of increasingly aggressive attacks.

In lower education (K-12), a lack of people/capacity, where schools did not have sufficient cybersecurity experts monitoring their systems at the time of the attack, was identified as the top operational root cause of an attack by 42%.[5] 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.

The Harris Federation attack,[6] which locked 50 schools out of its systems, left some staff scrambling to access Wi-Fi and contact emergency services. Critical infrastructure, from CCTV and door access systems to heating controls and payment portals, can be rendered useless, turning routine school operations into logistical nightmares.

[5] Sophos State of Ransomware 2025
[6] School cyber-attack affects 40,000 pupils' email

Reputational fallout and lost trust

Perhaps the most lasting damage is to a MAT's reputation. High-profile breaches erode parental confidence, leading to dropping enrolment numbers, a critical issue when funding is tied to student numbers. Regulatory repercussions, including GDPR fines and mandatory breach reporting, compound the damage. As one Sophos expert noted, **"No parent wants to send their child to a school that can't protect their data."**

A crisis that demands immediate action

With MATs 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. MATs 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.

MATs 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. MATs 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 entry points for network-wide compromise.

Equally critical is the implementation of multi-factor authentication (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 antivirus 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 such as RPA are asking for proof of regular cyber training and awareness within the schools and endpoint detection and response (EDR or XDR) assuming the MAT 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 school holidays, MATs' 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 go beyond detection with tailored intelligence and fast response times, which are increasingly crucial for insurance.

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,[7] 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 school networks. Implementing proper network segmentation can stop potential breaches, preventing an incident in one school from cascading across the entire trust.

[7] 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. MATs 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 as physical, printed forms and securely accessible digital documents.

The importance of reliable backups cannot be overstated in an era where 95% of attackers specifically target backup systems. MATs 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

MATs 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 a Cyber Essentials certification shouldn't be viewed as a complete security solution, it provides a valuable baseline framework and may reduce insurance premiums while demonstrating due diligence to regulators.

There's also significant value in collaborative defence approaches. MATs 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, MATs 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 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**

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

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

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

© Copyright 2025. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2025-07-28-WP (MP)