SOPHOS
Defeat Cyberattacks

Cybersecurity for Multi-Academy Trusts in England

A Sophos Whitepaper. July 2024

The changing face of education

Exactly how state education is overseen and delivered in England has gone through significant changes in recent times. Over half of pupils in state schools now attend academies[1]. In the 2022/23 academic year there were 10,176 academies and 4.9 million pupils attending academies, which equates to 41.6% of all schools and 54.4% of pupils[2]. Those figures are set to rise in line with government plans for all schools to convert to academies by 2030[3].

MATs benefit from greater financial efficiency, resource sharing and agility than their LEA-controlled counterparts. Pooling resources across multiple schools means MATs can achieve economies of scale, allowing for better allocation of funds towards educational resources and infrastructure improvements.

The changing face of technology in education

Education providers at all levels have a reputation for being digital laggards. It is, in some cases, an unfair reputation. Increasingly, technology underpins everything in education from both a teaching and operational perspective. This was highlighted during the COVID pandemic. When England entered lockdown in March 2020, education all but grinded to a halt. Thanks to technology adoption and the herculean efforts of education professionals, students and parents, many schools and academies were offering online lessons in time for the summer term. If the pandemic had happened just 10 years ago this ramping up of remote learning would have been implausible.

Moving forward, digital transformation will remain a top priority for academies. MATs are able to pool resources across locations and can collaborate more openly. All of which results in greater efficiencies, leading to faster more affordable technology deployment. However, the speed of such deployment against a backdrop of fragmented legacy systems can result in potential points of vulnerability for cyber-attacks.

Compounding the problem, MATs and all schools typically have an IT skills shortage. MATs can't afford large teams of people to work in IT and they certainly don't have time for proactive threat hunting. Teaching staff often have responsibility for how technology is used. Oftentimes those teachers might not be particularly tech savvy, but they find themselves responsible for liaising with hundreds of students online. Even in our post-lockdown world, teachers are increasingly delivering lessons using technology in the classroom, in addition to setting and marking homework remotely.

The use of technology is now, more than ever, critical for the delivery of education. But as MATs work to roll out the latest hardware and software they are faced with an uphill cybersecurity battle. Faster technology adoption, tighter budgets, fewer skilled IT people all point to major challenges ahead for MATs who would be mistaken to assume it will be business as usual when it comes to cybersecurity.

1 *What are School Trusts?*
2 *Improving schools' performance: Are multi-academy trusts the answer?*
3 *All schools to become academies by 2030*

The changing face of cybersecurity

More technology and greater fragmentation mean more points of weakness, and therefore more potential for successful cyberattacks. Education is seen as an easy target, the Sophos State of Ransomware 2023 study revealed that the rate of ransomware attacks in education continues to rise[4]. 80% of lower education providers and 79% of higher education providers reported that they were hit by ransomware in the last year, up from 56% and 64%, respectively, in our 2022 survey.

Without appropriate security MATs that take advantage of a consolidated, centralised, IT architecture run the risk of putting all their eggs in one basket. In 2022 the Scholars' Education Trust suffered the breach that affected six UK schools and over 4500 pupils[5]. Then in 2023 just before the start of the academic year, Maiden Erlegh Trust in Berkshire was targeted by a ransomware attack that took systems offline[6].

In the face of these challenges, many education organisations that were hit by ransomware paid the ransom to get their data back. The education sector is particularly exposed to the impacts of ransomware. According to the latest data from Sophos 59% of higher education organisations said they lost a lot of business/revenue, behind only business and professional services and media, leisure, and entertainment.

In the face of these challenges, many education organisations that were hit by ransomware paid the ransom to get their data back. In fact, the education sector has the third-highest rate of ransom payment (35%), behind energy, oil/gas and utilities (43%), and local governments (42%). However, those who paid only got back on average 68% of their data, leaving almost a third inaccessible, while just 11% got all their encrypted data back. In other words, paying the ransom doesn't really pay off.

In recent years, ransomware groups have become more professional, with well organised company-style structures and ransomware as a service (RAAS) affiliate schemes. It is not the case that threat actors only encrypt data and demand payments for decryption keys, but they increasingly exfiltrate valuable data and threaten to publish or sell it on the dark web.

Cybersecurity is a multi-layered threat

The threat posed by ransomware attacks is particularly damaging for MATs who handle student data and are financially responsible for the clean-up. The overall financial impact of ransomware is crippling for education organisations. Globally, lower education reported a mean recovery cost of $1.59M, and higher education reported a recovery cost of $1.06M. While these figures are below a cross-sector average of $1.82M, they're not unsubstantial.

In today's world, it is no longer enough to simply deploy antivirus software across networks and expect to be protected. Malware and hacking used to be two different threat landscapes; however, they have merged over the last five years. Attackers are stealthy – if IT teams don't play an active part in looking for signs of a breach, then cybercriminals can use (often legitimate) tools to enter and move around a network undetected, simply waiting for the right opportunity to strike.

'Hands-on attacks', where the adversary goes interactive within an IT estate, are becoming increasingly common and can unfold at lightning speed, quickly overwhelming staff. If this happens, it's crucial that an organisation has the expertise to respond rapidly at any time of day or night and bring in incident response services to assist

4 *The Sophos State of Ransomware 2023*

5 *Six UK schools hit by cyberattack on multi-academy trust*

6 *Cyber attack hits Wokingham's Maiden Erlegh School*

Barriers to transformative security

As MATs progress with their digital transformation plans, it will be result in more data being shared across networks and greater commonality of systems. This will result in more points of weakness and more cybersecurity risk as changes take place.

Headteachers and management teams are faced with three key, immediate challenges with digital transformation. First is the complexity of the existing or legacy platforms and software across a fragmented landscape. The second is a requirement to address security and compliance - the immediacy of this requirement can lead to quick fix solutions, which does not help with long term challenges. The third challenge is a lack of skills with new technologies such as cloud, AI and cybersecurity. Coping with these challenges can be a major headache for academy staff.

Furthermore, the move away from LES control and towards an environment that is more akin to the private sector can create a culture that strives for growth at some MATs. In turn, this can add to staff workload at a time when many academies are streamlining and centralising IT teams. Network managers working across academies therefore find themselves under increasing pressure.

MATs are increasingly looking towards managed service providers to help with these challenges. As the strategic importance of technology increases in line with its complexity, the role of the IT professional in education is moving up the value chain from implementation expert responsible for building, deploying and maintaining solutions to technology orchestrator responsible for long term goals and strategy.

Taking a long-term approach

Security, like insurance, is something you hope you never need, but absolutely must have in place from a compliance perspective and to manage risks. In fact, MATs would be well placed to work on the assumption that an attack will happen and ensure they have a tried and tested incident response plan that can be implemented immediately to reduce the impact of the attack. Complicating matters, threats are constantly evolving as criminals try new avenues of attack against the latest security. For instance, phishing is become ever more sophisticated and difficult to spot, especially in environments with high turnover, such as student intakes, using fragmented IT architecture.

Too many cyber breaches are caused by the inadvertent actions of users. Therefore, it is important that users are educated about the cyber risks they face and the safeguards in place to protect them. They should also understand their individual cyber security responsibilities, be aware of the consequences of negligent or malicious actions, and work with other stakeholders to identify ways to work in a safe and secure manner.

As individual staff members' machines are often the gateways for cybercriminals, all employees should complete Data Security Awareness Training[7], and participate in regular phishing simulations to raise awareness. At the very least you should check out the advice targeted at educators on the National Cyber Security Centre website[8].

The UK government provides additional guidance online about standards for schools and colleges regarding cyber security and user accounts, including information on safeguarding issues, the impact on student outcomes and much more[9]. This is not to be confused with the government-backed certification scheme Cyber Essentials – which is another valuable resource[10]. It is worth noting that guidance and certifications are nice to have in terms of preventative measures, but they are absolutely no guarantee of immunity.

7 *Data Security Awareness Training*
8 *National Cyber Security Centre*
9 *Meeting digital and technology standards in schools and colleges*
10 *About Cyber Essentials*

Avoiding breaches with the Protected Classroom

Taking a proactive approach to cybersecurity is vital. Schools are faced with the choice to either manage security themselves or outsource. Most do not have the budget, tools, people, and processes in-house to effectively manage their security programme around-the-clock while proactively defending against new and emerging threats. Furthermore, schools who do invest in cyber security solutions often fail to deploy them fully or use them to their full potential – significantly reducing their effectiveness and increasing the likelihood of a successful, but preventable breach.

The Sophos Protected Classroom offers comprehensive cybersecurity solutions tailored for the education sector. It provides robust protection against a range of cyber threats, including ransomware, malware, and phishing attacks. This solution is designed to safeguard students, educators, and administrative staff by leveraging advanced technologies such as Sophos Intercept X and Sophos Central.

Key features include:

- **Endpoint Protection**: Using Intercept X to prevent, detect, and respond to threats across all devices.
- **Firewall Protection**: Integrated solutions that secure cloud and hybrid networks.
- **Email Security**: Defends against phishing and impersonation attempts to protect critical information.
- **Cloud Security**: Secures workloads, data, and applications across AWS, Azure, Google Cloud, and Oracle environments.
- **Centralised Management**: Through Sophos Central, offering unified threat visibility and management.

Sophos also provides managed detection and response (MDR) services, ensuring continuous monitoring and proactive threat hunting by expert teams. This comprehensive approach helps educational institutions maintain a secure learning environment, allowing them to focus on educational priorities without being overwhelmed by cybersecurity threats.

More than just a notification service, the team's level of involvement is entirely within an school's control – from validating threats and removing the 'noise' of false positives to carrying out targeted actions on an IT team's behalf. Because these threat hunters are so familiar with malicious behaviour, once detected, the issue is often resolved within the hour.

Conclusion

With a continually changing threat landscape and limited budgets, securing MATs against cyber-attacks requires a collaborative team effort. By working together with your MAT, we provide the best opportunity to minimise security incidents and keep data safe as digitalisation continues apace.

Having a specialist team in your corner at all times – whether they're needed in the middle of the night, at a weekend or during school holidays – ultimately provides you with peace of mind, knowing you're doing all you can to keep education running and your staff, students and data safe.

The Protected Classroom with Sophos MDR offers different levels of support, giving schools options around the control over whether to retain or hand over responsibility to support teams. Plus, there's a wide variety of trusted Sophos security products that work side-by-side with MDR, all managed from within the Sophos Central platform for total visibility of your estate.

To learn more about Sophos MDR or to talk to a Sophos expert about the service for your ICS.

To learn more about Sophos MDR or to talk to a Sophos expert about the service for your ICS

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2024-07-08 (WP-PC)

SOPHOS