SOPHOS

Cybersecurity for Independent Schools in the UK

A Sophos Whitepaper. July 2024

The changing face of education

Approximately 5.9% of all schoolchildren in the UK attend private schools. The number of students at UK independent schools exceeds 554,000. This represents a 16.9% increase in pupils at independent schools compared to 1990[1]. The rise comes despite a 20% real term increase in average private school fees since 2010 and a 55% rise since 2003[2].

Inflation has driven a sharp increase in educational costs with school fees for the 2023/2024 academic year up by 8% on average, compared to the previous year[3]. Private school spend is 90% more than state school spend per pupil according to a report from the Institute for Fiscal Studies[4].

All of this additional revenue flowing through the independent school system makes the sector very attractive to cybercriminals. According to the Cyber Security Breaches Survey 2023 conducted by the UK government, 63% of private schools reported experiencing a cyber-attack, whereas only 50% of state schools reported such incidents[5].

These figures come amidst a global rise in cyber-attacks on educators. According to Sophos the rate of ransomware attacks in education continues to rise. 80% of lower education providers and 79% of higher education providers reported that they were hit by ransomware in 2023, up from 56% and 64%, respectively, in the 2022 survey[6].

A cyber-attack on any educator is a major concern. But for independent schools it could be a catastrophe. Any outage of services or data breaches could have massive ongoing financial ramifications.

1 Private School Statistics UK 2023 - Independent Schools
2 Tax, private school fees and state school spending
3 Private school fees soar and VAT threat looms – what does it mean for you?
4 English private school fees 90% higher than state school spending per pupil
5 Cyber security breaches survey 2023
6 The State of Ransomware in Education in 2023

The changing face of technology in education

Increasingly, technology underpins everything in education from both a teaching and operational perspective. And while independent schools have a reputation for being bastions of tradition, they are also early adopters of new technology and digital transformation is a top priority for most. However, the rapid adoption of new technology runs the risk of creating a fragmented landscape of legacy systems which can result in potential points of vulnerability for cyber-attacks.

Compounding the challenge, schools typically suffer from an IT skills shortage. Revenue is channelled into teachers' salaries and facilities; independent schools do not have 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 deployed and used. Often overburdened teachers might not be particularly tech savvy, but they find themselves responsible for liaising with hundreds of students online. Teachers are increasingly delivering lessons using technology in the classroom, in addition to setting and marking homework remotely.

The use of technology is critical for the delivery of education. But as independent schools 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 educators.

The changing face of cybersecurity

More technology and greater fragmentation mean more points of weakness, and therefore more potential for successful cyberattacks. At the same time, the rapid shift from classroom to online learning has piled additional work and pressures on IT teams.

Couple this with an increasing number of personal devices, either supplied by the schools or owned by individual pupils, and the result is a very challenging environment to control. Every school will have IT policies and guidelines in place for the proper use of devices and safe internet browsing, getting pupils follow those guidelines is another matter.

In the face of these challenges, many education establishments that were hit by ransomware paid the ransom to get their data back. According to Sophos, the education sector reported the highest ransomware attack rate across all industries in 2023.

As adversaries continue to hone their attack tactics, techniques, and procedures, defenders struggle to keep pace, resulting in increased encryption rates: over three-quarters of educational organizations (81% in lower education; 73% in higher education) hit by ransomware had their data encrypted. In addition, 27% in lower education and 35% in higher education reported that their encrypted data was also stolen.

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.

Cybercrime is a multi-layered threat

The threat posed by ransomware attacks is particularly damaging for schools who handle student data and are financially responsible for the clean-up. The reputational impact to a fee-paying school would be catastrophic if student details found their way onto the dark web.

The overall financial impact of ransomware is crippling for education organisations. For education providers operating in the private sector, ransomware has a major business impact. According to Sophos data 94% of lower education and 88% of higher education organisations hit by ransomware reported that they lost business/revenue as a result of the attacks.

This is likely due to many education organisations running outdated and fragmented IT infrastructures supported by understaffed IT teams. As a result, in the wake of an attack they are often forced to totally rebuild from the ground up, incurring major financial cost.

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.

Barriers to transformative security

As independent schools accelerate with their digital transformation plans, it will 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. Second is the 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 is a major headache for schools. The independent school sector is highly competitive and this culture for excellence and development can add even more pressure on staff at a time when many schools are streamlining and centralising IT teams. Network managers working across schools are finding themselves under increasing pressure.

Independent schools 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 risk. In fact, independent schools 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 has become more sophisticated and difficult to spot, especially in environments with high people 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.

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.

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

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 independent schools against cyber-attacks requires a collaborative team effort. By working together with your school, Sophos can 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.

Choose from Standard or Advanced Sophos MDR[11]– whatever you decide – you'll be safe in the knowledge that our dedicated security personnel will identify and eliminate threats before they can even become an issue.

To learn more about the Sophos MDR service visit our website or read our case studies and research.

11 Standard or Advanced Sophos MDR

2024-06-28 (WP-NP)

SOPHOS