Numbers Don't Lie: Cyber Security Risks Facing Schools in 2026/27

Cyber security in schools has moved from being a technical concern to becoming a whole school risk. The digital systems used by schools now support almost every part of education, from teaching and learning to safeguarding, finance, assessment, communications, premises management and parental engagement. When those systems are unavailable or compromised, the impact is no longer inconvenient but can affect the ability of a school to operate safely, protect personal information, meet statutory requirements and maintain teaching and learning.

The evidence from our recent cyber security assessments across over 100 primary and secondary schools shows progress but there are still gaps in the overall approach to risk mitigation. Some controls are now widely adopted. Staff cyber awareness training is in place in 82% of schools and infrastructure documentation is maintained in 75% of schools. Most schools, 79%, report that their backups include at least three copies of important data on at least two separate devices, with at least one copy held off site. These are positive signs and show that many schools have taken practical steps to improve resilience.

However, the same data also exposes significant weaknesses in the areas that matter most when a school faces a cyber incident. Only 48% of schools have understood and documented their greatest cyber risks, including the likelihood and impact on the school. Only 34% report that their SLT Digital Lead understands what data is currently being backed up, how often it is backed up and how it is being backed up. Only 43% of schools back up their cloud data and email, such as Microsoft 365 or Google Workspace. These findings suggest that many schools have technical tools in place but do not yet have the level of leadership assurance needed to understand whether those tools would protect them when under pressure.

Cyber security is no longer about whether a school has a firewall, endpoint protection or a backup system. It is about whether leaders understand the risks, responsibilities are clear, whether processes are tested and if the school can recover quickly when something goes wrong. The Department for Education's Digital and Technology Standards recognise this by placing cyber security alongside digital leadership and governance as part of the six core standards schools should be working towards by 2030.

The data suggests that this leadership dimension remains underdeveloped.

Only 13% of schools overall report that every term, the SLT Digital Lead reviews whether all digital technology is supported and licensed. In primary schools, the figure is 17%. In secondary schools, it falls to just 8%. This is one of the most important findings in the assessment data because it highlights a gap between operational IT management and strategic oversight. Schools may have systems that are working day to day, but too few appear to be reviewing them regularly at senior leadership level.

This matters because unsupported or unlicensed technology can become a silent risk. Old software, unmanaged devices, expired licences and unknown systems create opportunities for attackers. They can also weaken a school's ability to evidence compliance, respond to incidents or maintain continuity. The DfE's cyber security guidance includes keeping digital technology supported, licensed and up to date as one of the areas schools should address. In practice, this means that leaders need regular visibility of what is in use, who is responsible for it and whether it remains secure.

The picture is stronger when looking at technical documentation for local infrastructure. Three quarters of schools have up to date documentation for infrastructure, with secondary schools performing slightly better at 80% compared with 74% of primary schools. This suggests that traditional infrastructure is relatively well understood in many schools. Yet cloud services documentation is weaker, with only 53% of schools overall reporting that it is up to date.

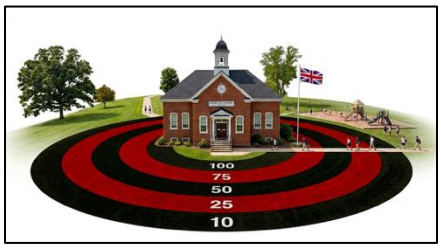
This difference reflects a wider shift in school technology. For many years, cyber security focused heavily on servers, local networks and devices within the school building. That world has changed with schools now relying

heavily on cloud email, cloud storage, online learning, safeguarding systems and externally hosted applications. As more services migrate to the cloud, moving outside the school network, the security focus must move with them. A well documented server estate is still valuable, but it does not provide enough assurance if the school lacks a clear view of cloud services, user access, data locations and backup arrangements.

Schools Remain a Target

Schools hold large amounts of sensitive data, including pupil records, staff records, safeguarding information, medical details, financial data and parent contact information. They also depend heavily on access to systems during the school day. An attack that disrupts access to email, registers, safeguarding records or finance systems can create immediate operational pressure. For criminals, that pressure can increase the chance that victims will make rushed decisions, especially in ransomware or extortion cases.

Schools also operate in a difficult financial and resource environment. Unlike large corporate organisations, many schools and trusts do not have large IT budgets or large cyber security teams. IT staff are often responsible for a broad range of services, from classroom support to network management, procurement, device repairs and strategic planning. In smaller schools, IT support may be outsourced or shared across several sites. This does not mean schools lack expertise, but it does mean there is often limited capacity for proactive cyber improvement.



Incident Planning

The assessment data shows that many schools recognise the need for incident planning, but there is still work to do. Overall, 63% of schools report that they have put a cyber response plan in place. Primary schools are ahead at 71%, while secondary schools sit at 51%. This means that more than one third of schools overall do not yet have a cyber response plan in place. The gap is especially concerning in secondary settings, where technology estates are often larger, user numbers are higher and the complexity of IT services is much greater.

In addition to being a key requirement of the RPA, the most common cybersecurity insurance provider in schools, a cyber response plan is critical. It should explain what steps are to be taken, who makes decisions, who contacts key stakeholders, how systems are isolated, how evidence is preserved, how safeguarding risks are managed and how recovery is prioritised. It should include routes for reporting incidents both internally and externally. The DfE cyber security standard includes reporting cyber attacks as one of the areas schools and colleges should address. Without a clear plan, valuable time can be lost during the early stages of an incident, when calm decision making matters most.

The strongest organisations treat cyber incident response in the same way they treat fire safety or safeguarding escalation. They do not wait for an incident to decide who is responsible. They document the process, train the relevant people, test the plan and review it after lessons are learned. Schools should take the same approach. A short, practical response plan that is understood and rehearsed is far more valuable than a long technical document that is rarely read.

Managing Access

Identity and access control remains another key area of concern. Only 59% of schools report that MFA is enabled for all staff accounts. Secondaries perform slightly better at 63%, with primaries at 56%. This means that around four in ten schools still do not have MFA enabled for all staff accounts. Student MFA is far less common, with only 6% of schools enabling it where verification does not need to be completed on a mobile phone. In addition, only 23% of schools report that access to the firewall's administrative interface is protected with MFA.

These figures represent one of the clearest risk areas in the data. Most cyber attacks target user accounts rather than physical infrastructure. A compromised staff account can provide access to email, files, shared data, cloud applications and internal communications. If that account has additional privileges, the risk increases further. Some say that MFA is not a perfect control but Microsoft data claims it reduces the likelihood that a stolen password alone will lead to unauthorised access by over 99%.

The firewall administration figure is particularly important. Schools often think of their firewall as a key protective barrier, but if administrative access to that firewall is not strongly protected, the control itself becomes more vulnerable. Only 29% of primary schools and 16% of secondary schools report that the firewall administrative interface is protected with MFA. Given the importance of firewall management, this is a priority area for improvement.

Keeping Systems Up To Date

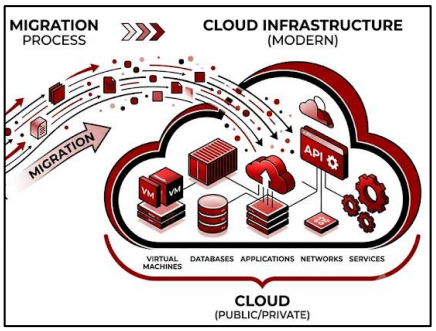
Patching is another area where the sector shows partial progress but not yet enough consistency. Overall, 59% of schools report that they install security updates to operating systems, applications and firmware, including configuration changes, within 14 days of release.

Schools face real challenges in patch management. Some systems are difficult to update during term time. Some curriculum topics depend on older versions of software. Some infrastructure may require supplier involvement. Yet attackers often move quickly once vulnerabilities become public. A patching process does not need to be perfect, but it does need to be risk based, visible to leaders and supported by accurate asset information. The lower rate of termly SLT review of supported and licensed technology suggests that many schools may not have the governance process needed to challenge patching risks at the right level.

Keeping Data Secure

Backups present one of the most interesting contrasts in the data. On the surface, backup practice appears reasonably strong. Overall, 79% of schools report that they have at least three backup copies of important data on at least two separate devices, with at least one copy held off site. This is encouraging, yet only 34% of schools report that their SLT Digital Lead knows what data is being backed up, how often it is backed up and how it is being backed up. Then, only 43% back up cloud data and email.

This means that many schools may have backup solutions but lack leadership assurance. That distinction is critical. In a ransomware incident, the question is not simply whether a backup product exists. Leaders need to know which systems can be restored, how quickly they can be restored, how much data could be lost, whether cloud data is included and whether backups have been tested. If these questions cannot be answered before an incident, they will be much harder to answer during one.



Cloud backup is a particular concern. Many schools now rely on Microsoft 365 or Google Workspace for email, document storage, teaching and collaboration. There is sometimes an assumption that cloud data is automatically protected by the provider in all circumstances. Sadly, this is rarely true and the user (the school) is normally responsible for maintaining a backup of their own data. Schools are still responsible for understanding how their data is protected, what recovery options exist and whether additional backup arrangements are needed. The DfE standards include developing and implementing a data backup plan and reviewing it annually. The assessment data suggests that this should be a priority, especially as cloud use continues to grow.

Cyber Security Awareness

Staff awareness is one of the stronger areas in the assessment data. Overall, 82% of schools have cyber security awareness training in place for staff. Secondary schools are slightly ahead at 88%, with primary schools at 81%. This is positive and reflects growing recognition that people are central to cyber resilience. Phishing, social engineering, weak passwords and unsafe handling of information remain common routes into schools. Staff who understand the risks are more likely to spot suspicious activity and report concerns early.

Targeted Recommendations

The most important conclusion from the data is that school cyber security is not consistently adopted and deployed. There is significant progress being made, but large gaps still remain and these place schools are risk. The weaker areas are the ones that determine whether cyber security is embedded as a leadership discipline.

DLT Digital Lead

Every school should have a named SLT Digital Lead with a clear responsibility to review cyber risk, supported technology, licensing, backups, MFA, patching, response planning and awareness activity. This does not mean senior leaders need to become technical specialists. It means they need to ask the right questions, understand the answers and ensure that risks are recorded and acted upon.

Cyber Risk Assessments

Schools should complete and review a cyber risk assessment at least annually, with termly leadership review. With only 48% of schools currently documenting their greatest cyber risks, this is one of the most important areas for improvement. A school cannot manage cyber risk effectively if it has not identified what the main risks are, how likely they are to occur and what impact they would have. The DfE standards specifically include conducting a cyber risk assessment annually and reviewing it every term.

Close the MFA Gap

MFA should be in place for all staff accounts, administrator accounts, remote access services, cloud platforms and firewall administration. Where student MFA is appropriate and can be implemented without requiring mobile phone verification, schools should explore safe and practical options. MFA should be seen as a core protection for identity, not an optional enhancement.

Strengthen Backup Assurance

Schools should not only ask whether backups exist. They should ask what is backed up, how often it is backed up, where it is stored, whether it includes cloud data and email, how quickly it can be restored and when recovery was last tested. This must include all data, especially that stored in the cloud and should be reported in plain English to senior leaders and governors. Backup testing should be treated as a continuity exercise, not merely a technical task.

Incident Response

Every school should have a clear cyber response plan that explains roles, communication routes, escalation, containment, recovery and reporting. It should be short enough to use during a crisis and clear enough for non-technical leaders to follow. It should be reviewed regularly and tested through simple scenario exercises. Templates are available from the RPA website.

As schools look ahead, the risk landscape will not become simpler. Cloud reliance will continue to grow. Attackers will continue to target identities. Artificial intelligence will make phishing and social engineering harder to detect. Financial pressure will continue to challenge investment decisions. At the same time, schools will continue to become ever more dependent on digital systems to deliver teaching and learning, manage safeguarding and communicate with their communities.

The evidence from the 128 school assessments in the dataset shows that schools have a solid foundation to build on. There is clear progress in documentation, awareness and backup practice. Yet the areas requiring improvement are significant and should not be deferred. Too many schools still lack documented risk assessments. Too many have gaps in MFA. Too many lack leadership visibility of backups and too few are reviewing supported and licensed technology every term.

Cyber security risk mitigation in UK schools is therefore at a turning point. The next stage of maturity will not be achieved simply by buying more technology. It will come from better governance, clearer ownership, stronger assurance and more consistent follow through. Schools that make cyber security part of normal leadership practice will be better placed to prevent incidents, respond calmly when they occur and recover with less disruption.

About Virtue Technologies

Virtue Technologies is an education-focused IT company with nearly two decades of experience partnering with schools to deliver tailored technology solutions. Established in 2006, the company has become a leading provider of IT services for Primary, Secondary Schools and Multi Academy Trusts. Their key areas of expertise are Support, Cyber Security, Cloud Solutions and Classroom Productivity.

With a clear commitment to enhancing educational outcomes through technology, Virtue Technologies collaborates closely with academic institutions to understand their unique needs and challenges. The company emphasises building long-term partnerships, ensuring that each solution not only aligns with current requirements but also anticipates future growth. Their dedicated team of professionals stays abreast of technological advancements, allowing them to introduce innovative practices and resources into classrooms efficiently. Over the years, Virtue Technologies has earned a strong reputation within the educational sector for reliability, adaptability and exemplary customer service. By focusing on continuous support and professional development, they empower educators and

administrators to make the most of their IT investments, fostering enriching learning environments for students across all levels of education.

About the Author

Will Stead has over 35 years of experience in IT management and leadership, spending the last 15 years specialising in the education sector, supporting schools and Multi Academy Trusts across the UK.

Will's expertise lies in developing and implementing IT strategies tailored for both individual schools and MATs. He works directly with school leadership teams and IT departments to create strategic plans that drive digital transformation, improve classroom productivity and ensure robust cybersecurity practices. His approach is highly collaborative, focusing on building strong relationships and trust with stakeholders to deliver technology solutions that are both effective and

sustainable.

Contacting Virtue Technologies

01695 731 233

info@virtuetechnologies.co.uk

www.virtuetechnologies.co.uk