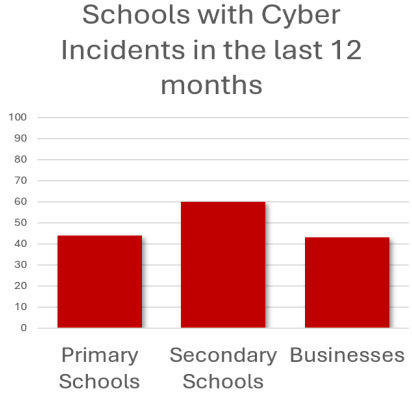
Cyber Resilience in Education: Insights from the 2025 UK Cybersecurity Breaches Survey

The 2025 Cyber Security Breaches Survey, published by the Department for Science, Innovation and Technology, offers a comprehensive picture of how UK organisations are managing cyber threats. In particular, the companion report on educational institutions provides important insights into how primary and secondary schools are faring. While there is encouraging evidence of growing awareness and leadership engagement, the survey also highlights persistent vulnerabilities, especially in technical implementation and the uptake of external guidance.

In this paper, we look at the key findings from both reports with a focus on schools. Where relevant, we reference the Department for Education's Digital and Technology Standards for Schools and Colleges, which provide a benchmark for cybersecurity governance and infrastructure across the education sector.

Cyber Incidents in Schools

The report shows that schools continue to experience a high level of cyber threats, with 60% of secondary schools and 44% of primary schools reporting at least one identified cyber breach or attack in the past 12 months. This is higher than the average across UK businesses (43%).



Compared to 2024, these rates have remained relatively stable, suggesting that while awareness is increasing, the underlying threat environment remains active. Secondary schools are especially exposed, likely due to their larger IT estate, complexity of solutions and numbers of users.

Common Threat Types

Among schools that experienced a breach or attack, the most frequent threat was phishing, which was reported by 89% of schools with identified incidents. Other types of attacks included impersonation attacks (50% of secondary schools), malware and viruses (22% of secondaries) and Denial of Service (DoS) attacks (10% of secondaries).

Phishing's dominance is in line with broader industry trends, but the relatively high proportion of impersonation and malware cases highlights the importance of training and layered security controls in schools, especially for staff and students.

Leadership and Governance

Schools continue to place a strong emphasis on cybersecurity at Senior Leadership level with 98% of primary schools and 95% of secondary schools reporting it to be a high priority for the Senior Leadership. This far exceeds the business average (72%) and shows that school leadership is aware of the strategic importance of cyber resilience.

It is also encouraging to see the growing practice of formal reporting to governing bodies. 73% of primary and 67% of secondary schools provide regular cyber risk updates to their Board of Governors. These numbers are up from the previous year, indicating improving governance maturity.

These trends closely align with the DfE standards, which require leadership to designate a Senior Digital Lead and maintain clear oversight of digital risks, including cybersecurity.

Risk Identification and Technical Controls

Risk assessment is increasingly embedded in schools' operations, with 84% of primary and 86% of secondary schools carrying out cybersecurity risk identification in the past year. This is significantly higher than the business average (49%).

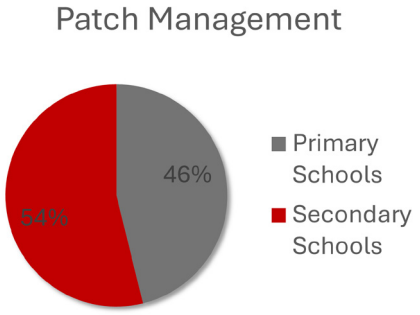
In terms of technical controls, most schools are implementing core measures such as:

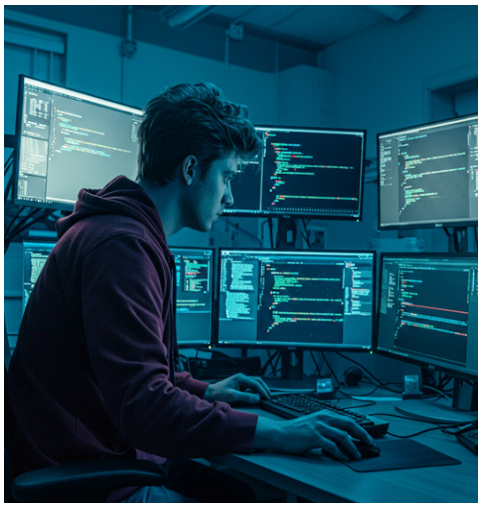
- firewalls
- anti-malware software
- password protection and access controls

However, some areas still need improvement:

- only 48% of primary and 56% of secondary schools have formal patch management policies
- penetration testing was conducted by 23% of primary and 31% of secondary schools - still relatively low
- virtual private networks (VPNs) and guest Wi-Fi networks are more common in secondary schools, but their usage in primary settings remains inconsistent

The DfE standards specifically call for up-to-date patching practices and segmented, secure networking infrastructure. The findings suggest that while foundational controls are in place, more advanced practices are uneven, especially in smaller or less technically resourced schools.





Incident Response and Continuity Planning

Having a well-prepared response to cyber incidents is critical and in addition to the DfE's guidance, having an incident response plan is also a requirement of the RPA's cyber-insurance. The survey shows good progress for schools, with 71% of primary schools and 74% of secondary schools having formal incident response plans. It is also encouraging to see that 73% of primary and 77% of secondary schools have business continuity plans that account for cybersecurity incidents.

Most schools also followed good practice during real-world incidents by informing governors, assigning roles and responsibilities and maintaining incident logs.

These actions align well with the DfE's standards, which emphasise both prevention and resilience. However, the absence of incident response plans in about a quarter of schools suggests further work is needed to embed preparedness more widely.

External Support and Supplier Assurance

While internal governance is improving, schools appear less engaged with external frameworks and support. Awareness and use of government cyber guidance (e.g. from the NCSC, Cyber Essentials, 10 Steps to Cyber Security) remains low and only 5–14% of primary schools and 11–20% of secondaries reported using this guidance.

In addition, only 26% of primary and 38% of secondary schools reported formally assessing cyber risks within third-party suppliers. This is a concern given the rise of supply chain-related attacks across sectors.

Staff Training and Culture

Cultural factors also influence cyber risk. According to the findings, 96% of primary and 95% of secondary schools now provide cyber awareness training to staff. However, training for governors and non-teaching staff is less consistent.

Interviews in the report suggest that training can often be ad hoc or driven by a reactive response to specific incidents. Some IT Leads noted frustration over low engagement levels with refresher materials, especially when they are not mandatory.

The RPA mandate that all users complete the National Cyber Security Centre's awareness training for schools, which is free as part of its cyber insurance cover. The DfE also encourages regular, role-specific training as part of a whole-school approach to digital safety.

The Role of the DfE Standards in Driving Improvement

The DfE's Digital and Technology Standards for Schools and Colleges serve as a useful benchmark throughout this discussion. While they are not statutory, they do help schools assess their progress in areas such as:

- leadership and governance
- technical security
- resilience and recovery planning

The survey data shows many schools partially meet these standards. For example:

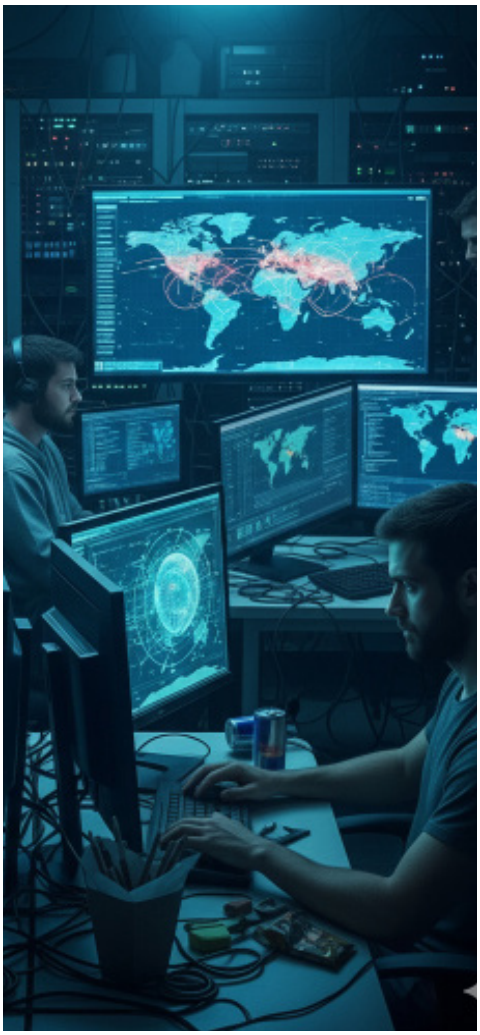
- board-level cyber oversight is widespread
- business continuity planning is well established
- core security measures (firewalls, malware protection, backups) are in place

However, the standards also highlight gaps:

- patch management and third-party assurance remain weak points
- asset registers and documented policies are not universal
- awareness of external support tools and frameworks is low

Department for Education

To bridge these gaps, schools could make greater use of the external assessments and planning tools (such as Virtue's Cyber Assessments), which are designed to align operational practice with the standards.



Summary

The 2025 Cybersecurity Breaches Survey paints a picture of a school sector that is increasingly aware of cyber threats and is actively taking steps to address them. Senior leaders are engaged, risk assessments are becoming routine and incident response is more structured than in previous years.

Yet challenges remain. Technical practices such as patching and supplier assurance are still underdeveloped in many educational settings, particularly in primary schools. Awareness and use of national guidance and certification schemes remains low, limiting the sector's overall cyber maturity.

The DfE standards offer a roadmap for improving consistency and robustness across the board. As schools continue to expand their use of digital tools and platforms, aligning day-to-day practice with these standards will be essential in reducing risk and maintaining trust in digital education environments.

Continued investment in training, technical support and policy implementation will help close the gap between strategic intent and operational execution. With a steady focus on both culture and controls, schools can move toward a more secure and resilient digital future.

Additional Reading:

- Cyber Security Breaches Survey 2025 – Click here
- Cyber Security Breaches Survey 2025 (Education Institutions Findings) – Click here
- DfE Digital and Technology Standards in Schools and Colleges – Click here

About Virtue

Virtue Technologies is an education-focused IT company with nearly 20 years of experience working collaboratively with Schools to deliver fit-for-purpose technology solutions. Founded in 2006, we have gone on to become a leading provider of IT solutions to Primary and Secondary Schools, Multi Academy Trusts, Further Education Colleges and Universities.

About the Author

Will Stead works closely with Schools and Multi Academy Trusts to support the development of IT and Cybersecurity Strategy and Plans. He has over 35 years of experience in the IT industry, with the last 15 years in education.