Cyber attacks on education are not just an IT problem, warns Derbyshire cyber security specialist

derbyshiretimes.co.uk/your-world/cyber-attacks-on-education-are-not-just-an-it-problem-warns-derbyshire-cyber-security-specialist-8671826

Phil Bramley June 11, 2026

Kevin Walker of Black Swan Cyber Security Solutions reviewing cyber incidents | Black Swan Cyber Security Solutions

Black Swan Cyber Security Solutions says attacks on schools, colleges and universities can affect safeguarding, learning, payroll, parent communication and public trust.
A Derbyshire cyber security specialist is urging education leaders to treat cyber resilience as a business continuity issue, following recent reports of a cyber attack affecting the University of Nottingham.

The University of Nottingham has confirmed that a cyber criminal group accessed personal data held in its student records system. Reports say the incident may involve current students and alumni, with the university notifying those affected and reporting the matter to Report Fraud and the Information Commissioner's Office.

Kevin Walker, founder of Black Swan Cyber Security Solutions in Chesterfield, says incidents like this show how quickly cyber security moves beyond IT.

Kevin Walker - Black Swan Cyber Security Solutions | Black Swan Cyber Security Solutions

“When people hear ‘cyber attack’, they often picture a technical problem,” said Kevin. “But in education, it becomes a safeguarding, continuity and communication problem very quickly.

“If a school, college or university loses access to its systems, it is not just an inconvenience. It can affect registers, safeguarding notes, parent contact details, payments, lessons, exams, payroll and confidence. That is why cyber security has to be treated as part of business continuity, not something bolted on to IT.”

The latest Government Cyber Security Breaches Survey found that education providers continue to face a high level of cyber risk. In the 12 months before the survey, 49% of primary schools, 73% of secondary schools, 88% of further education colleges and 98% of higher education institutions identified a cyber breach or attack.

Kevin, who has over 20 years’ experience supporting education IT, says schools and colleges should avoid panic, but take the warning seriously.

“Most education settings are not ignoring cyber security,” he said. “They are trying to manage it alongside budgets, staffing pressure, compliance, safeguarding and the daily job of keeping learning going.

“The important question is not whether they care. It is whether they have tested the things they would rely on during an incident.”

Black Swan Cyber Security Solutions is encouraging education leaders, governors and business managers to ask practical questions, including:

- When did we last test our backups?
- Could we restore our most important systems quickly?
- Is multi-factor authentication in place for key accounts?
- Are Microsoft 365 and email accounts being monitored for suspicious access?
- Do staff know how to report a suspicious email or login prompt?
- Does our incident response plan say who does what and when?
- Are cyber risks included in business continuity planning?

Kevin added: “A calm response does not happen by accident. It comes from planning, testing and making sure people know what to do before something goes wrong.

“Education cyber security should not be about blame or scare tactics. It should be about protecting learning, safeguarding information, reducing downtime and giving leaders clear evidence that the right controls are in place.”

Black Swan Cyber Security Solutions provides cyber resilience reviews for schools, colleges and small organisations. These include backup checks, Microsoft 365 security