Digital Security
Progress. Protected.

REPORT

Cybersecurity in Education 2025:

Securing the Future – An ESET Report

Progress. Protected.

Introduction

With cyber-attacks targeting educational institutions at an alarming rate, safeguarding sensitive data and maintaining operational continuity has never been more critical. This report explores the cybersecurity landscape in the UK education sector, drawing on recent research conducted by ESET (via Censuswide) and government reporting, to uncover key vulnerabilities, risks and opportunities for improved resilience.

Executive Summary

ESET's research reveals that 73% of educational institutions have experienced at least one cyber attack or breach in the past five years. Complementing this, the UK Government's 2025 survey indicates that secondary schools, further education colleges and higher education institutions are more likely to experience breaches than businesses overall in the UK. Despite the evident risks, many institutions lack fundamental cyber protections and face significant challenges related to budget restrictions, insurance adoption and preparedness for AI-driven threats.

Key Research Findings

→ CYBERATTACK EXPOSURE

According to government data, in the past 12 months, 60% of secondary schools, 85% of further education colleges and 91% of higher education institutions reported experiencing a cyber attack. These figures are notably higher than the 43% reported across UK businesses overall.

73% of institutions reported at least one cyber incident in the last five years according to our research, 20% of which experienced three or more breaches. Among higher education institutions, 30% experienced cyber breaches on a weekly basis, indicating a persistent threat landscape.

→ CYBER INSURANCE AND BUDGET CONSTRAINTS

Research highlights the critical challenges related to cyber insurance coverage and budgetary constraints, which may hinder the ability to effectively manage evolving cyber threats.

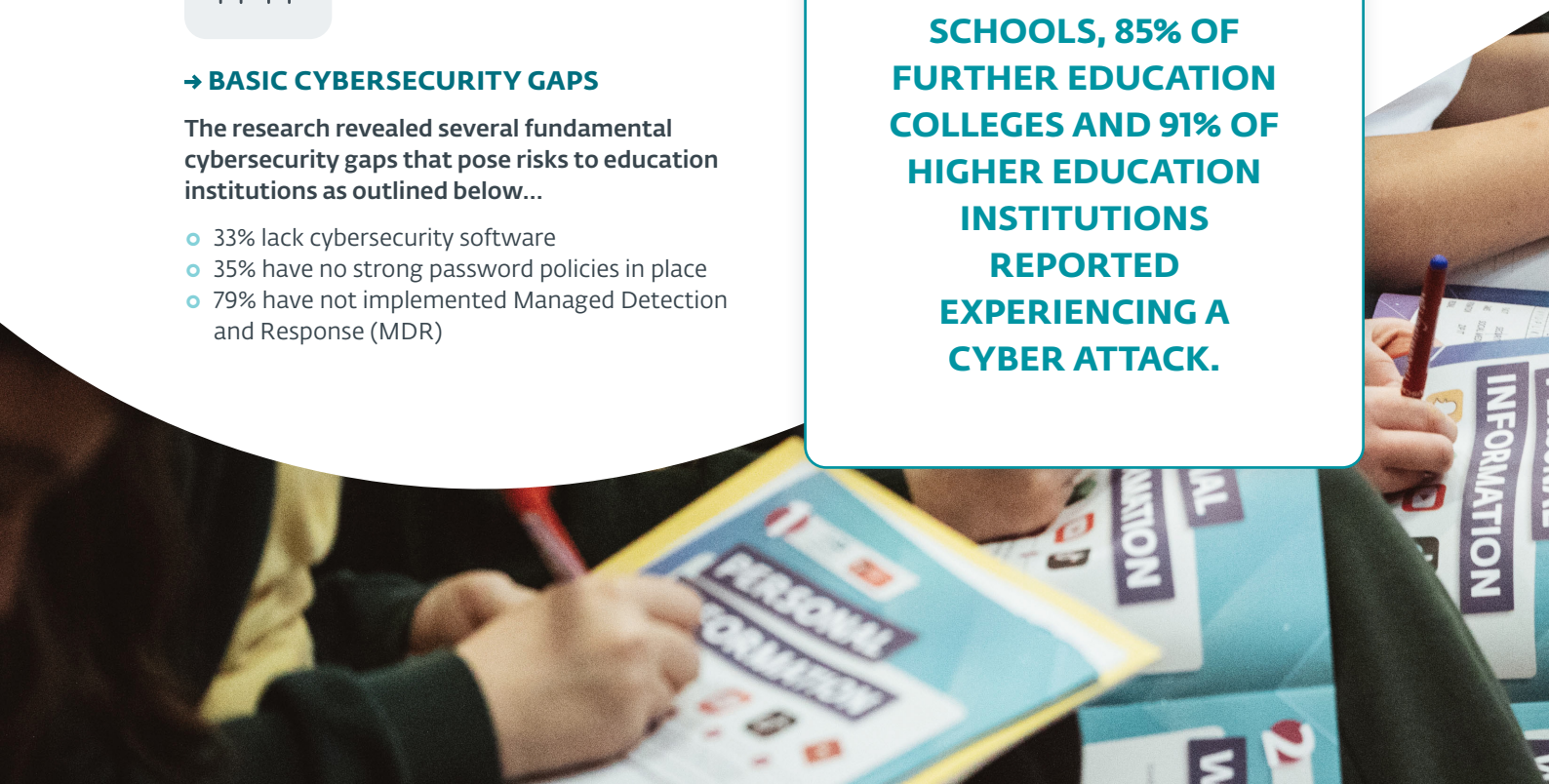
- Only 44% of primary and 36% of secondary schools have cyber insurance
- 7% of institutions report having no annual cybersecurity budget
- 21% feel unprepared to deal with AI-driven cyber threats

→ BASIC CYBERSECURITY GAPS

The research revealed several fundamental cybersecurity gaps that pose risks to education institutions as outlined below...

- 33% lack cybersecurity software
- 35% have no strong password policies in place
- 79% have not implemented Managed Detection and Response (MDR)

60% OF SECONDARY SCHOOLS, 85% OF FURTHER EDUCATION COLLEGES AND 91% OF HIGHER EDUCATION INSTITUTIONS REPORTED EXPERIENCING A CYBER ATTACK.



→ BARRIERS TO CYBER INSURANCE ADOPTION

Key barriers to the adoption of cyber insurance were identified, with institutional leaders expressing a range of concerns that influence their decision-making...

- 37% prioritise direct cybersecurity investments over insurance
- 33% worry about payout reliability
- 32% cite unclear policy terms
- 28% believe insurance is too expensive
- 18% don't understand its value

21%

feel unprepared to deal with AI-driven cyber threats

→ TOP CYBER THREATS

Key barriers to the adoption of cyber insurance were identified, with institutional leaders expressing a range of concerns that influence their decision-making...

- 37% prioritise direct cybersecurity investments over insurance
- 33% worry about payout reliability
- 32% cite unclear policy terms
- 28% believe insurance is too expensive
- 18% don't understand its value

According to the government report, phishing remains the most prevalent threat, with 97% of further and higher education institutions and 89% of primary and secondary schools encountering such attacks.

→ AWARENESS AND READINESS

While there is a generally positive perception of staff cybersecurity awareness, the data indicates a continued emphasis on strengthening readiness through enhanced training and expanded toolsets.

- 76% believe staff have good cybersecurity awareness
- 55% plan to increase staff training
- 51% will expand cybersecurity tools in the next year

51%

will expand cybersecurity tools in the next year

"It's fantastic to see that the education sector is increasingly taking the threat of cyber attacks seriously with clear progress being made to withstand the ever-changing threat landscape. This commitment is a really encouraging step in the right direction and will proactively improve defences in schools across the UK. Naturally, however, there's still more that could be done. Not all schools remain fully prepared and without all the right measures in place, some could be vulnerable to a cyberattack. It's therefore vital that the entire sector continues to build on this momentum to ensure every school is equipped to protect itself from evolving cyber threats."

JAKE MOORE,
GLOBAL CYBERSECURITY ADVISOR

→ IMPACT OF CYBER INCIDENTS

Approximately 40% of further and higher education institutions reported experiencing negative outcomes from cyber breaches, such as compromised systems and accounts used for criminal activity.

The average ransom demand for schools has escalated to £5.1 million, with recovery costs nearing £3 million according to the Sun newspaper.

The average ransom demand for schools has escalated to

£5.1 million

→ SUPPORT NEEDS

The findings underscore a strong interest in managed cybersecurity services. Just because the school bell rings at 3pm doesn't mean cybercriminals have punched out for the day. They are 'always on'. ESET MDR is a 24/7 cybersecurity service that uses a combination of AI-powered automation and human expertise, along with comprehensive threat intelligence, to achieve unmatched threat detection and rapid incident response.

- 77% see value in managed cybersecurity services
- 47% would need evidence of financial impact to secure more budget from leadership

77%

see value in managed cybersecurity services

ESET MDR is a 24/7 cybersecurity service that uses a combination of AI-powered automation and human expertise, along with comprehensive threat intelligence, to achieve unmatched threat detection and rapid incident response.

Recommendations

Cybersecurity should be viewed by educational institutions as a strategic investment not simply a technical or IT-related expense. With schools, colleges and universities increasingly reliant on digital platforms for teaching, administration and communication, protecting these systems must be integrated into institutional planning at the highest level.

Investing in proactive measures today will help ensure operational continuity, maintain trust within the school community and protect sensitive data against a growing array of cyber threats. Given the high prevalence of phishing attacks, institutions should implement advanced email filtering solutions and conduct regular awareness training for staff and students.

- Ensure timely updates and patches to all systems to mitigate vulnerabilities, especially in primary schools where patching standards lag.
- Establish and regularly test incident response plans to ensure readiness in the event of a cyber incident.
- Implement rigorous supply chain risk assessments and monitoring to safeguard against third-party vulnerabilities.
- Provide ongoing, mandatory cybersecurity training for all staff and, where feasible, for students to foster a culture of security awareness.
- Recognise cybersecurity as a critical investment area, ensuring adequate funding for necessary tools, training and insurance.

ACTION	IMPACT
Allocate budget to cybersecurity	Strengthens protection and reduces risk
Adopt MDR or managed support	Enables 24/7 threat monitoring and faster response
Train staff and students regularly	Builds a culture of cyber awareness
Explore cyber insurance options	Mitigates financial losses from breaches
Create a robust response plan	Ensures continuity during cyber events

Conclusion

The education sector is facing a cybersecurity crossroads. ESET's findings show that although awareness is growing, substantial action is still required. By combining proactive security investments, robust training, managed services and insurance, UK educational institutions can better protect their operations, data and students from today's escalating cyber threats. Safeguard your school, college, or university with ESET.

What ESET partners think...

> "As a Managed Service Provider for Education, it is critically important for us to have rigid security in an ever more challenging environment. ESET's been great, we never had any issues for all these years and scalability has been very straightforward. Technical support is second to none. We normally communicate with our account manager on a weekly basis. We even co-hosted customer-facing events where ESET helped with our budget. Overall, we mostly enjoy consistency and reliability so we can focus on what we do best - ICT for our schools."
>
> **IMRAN KHAN,**
> **SERVICES DIRECTOR, MGL**

Sources

- Censuswide ESET research
- Government stats