Cybersecurity
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 and accelerating rate, safeguarding sensitive data and ensuring operational continuity has never been more critical. Educational institutions are now prime targets for both sophisticated cybercriminals and nation-state actors. In Q2 2024, Microsoft ranked the education sector as the third most targeted globally, while ESET researchers observed heightened Advanced Persistent Threat (APT) activity from groups aligned with China, North Korea, Iran and Russia.

A perfect storm of vulnerabilities, including porous networks, legacy technology, limited cybersecurity budgets and a large, transient user base, makes the sector especially attractive to attackers. In the UK alone, 73% of secondary schools and nearly all universities reported serious security breaches in the past year, a rate significantly higher than in the business sector.

ESET's recent research (via Censuswide) and UK government reporting reveal further troubling trends: 73% of institutions have experienced at least one cyber attack in the last five years. Financial gain remains the dominant motive behind these attacks (88%), but espionage accounts for a growing share (18%), especially at institutions involved in sensitive research.

Without a robust, prevention-first cybersecurity strategy, schools, colleges and universities risk not only financial and reputational damage, but also severe disruption to their core mission of teaching, research and community service. For many institutions facing budget constraints and IT staffing shortages, fully automated, real-time security solutions are no longer optional, they are essential.

Executive Summary

In 2023, the University of Manchester experienced a major ransomware breach that targeted critical systems supporting healthcare-related research. Sensitive data was exfiltrated, triggering regulatory investigations and forcing the suspension of several academic operations. This high-profile incident is emblematic of a broader crisis across the education sector.

ESET's research reveals that 73% of educational institutions have experienced at least one cyberattack or breach in the past five years. The UK Government's 2025 survey reinforces this trend, showing that secondary schools, further education colleges and higher education institutions are more likely to suffer breaches than UK businesses overall. Yet, despite these evident risks, many institutions still lack essential cybersecurity protections and continue to face challenges related to limited budgets, low cyber insurance adoption and insufficient 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.

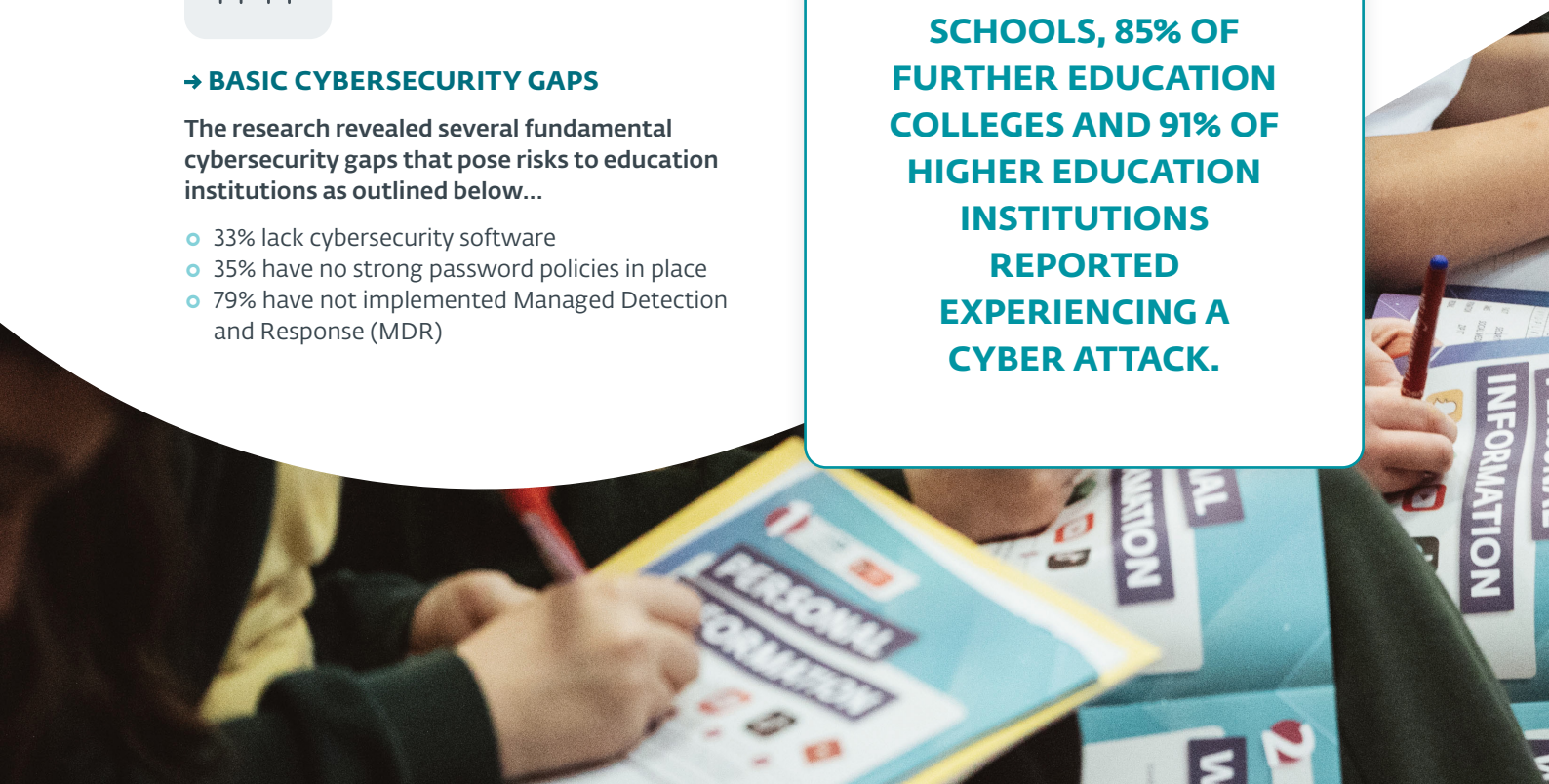
- Only 44% of primary and 36% of secondary schools have cyber insurance
- 7% of institutions report having no annual cybersecurity budget
- 21% feel unprepared to deal with AI-driven cyber threats

→ 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.

→ ESET SOLUTIONS

Educational institutions need cybersecurity solutions that are not only powerful, but preventive, automated and practical, adapting to budget constraints, IT staffing levels, and fast-changing threat landscapes. ESET's PROTECT Platform offers a unified, scalable ecosystem that helps schools and universities prevent, detect and respond to threats efficiently.

The platform includes modern, fully automated Endpoint Protection with ransomware shields and remediation, and behavioural detection. ESET Cloud Office Security (ECOS) adds an essential layer of defence for Microsoft 365 and Google Workspace applications, minimising risk from phishing, business email compromise and malicious file sharing within collaboration tools. It also includes Anti-spoofing and Homoglyph protection, identifying threats that traditional filters or human users may overlook.

Keeping pace with best practices like patching, encryption, and policy enforcement can overwhelm limited IT teams. The ESET PROTECT Platform helps by centralizing and automating core security and IT management tasks, including Vulnerability and Patch Management (V&PM) to swiftly close known gaps. ESET Secure Authentication delivers simple, scalable MFA, helping overcome weak password habits and preventing unauthorised access across student, staff and admin accounts. Encryption tools assist with compliance mandates under GDPR, FERPA and HIPAA.

For institutions with overstretched IT departments or limited in-house expertise, ESET's Managed Detection and Response (MDR) provides fully managed 24/7 protection and expert threat hunting, taking over the technical back-end so internal teams can focus on strategic and high-value tasks rather than drowning in security alerts. MDR directly addresses the challenges of today's education threat landscape, broad attack surfaces, diverse entry points and persistent targeted campaigns, all with the benefit of 24/7/ 365 protection at a fraction of the cost of building internal capabilities. Whether a small district or a large research university, ESET's solutions scale intelligently and affordably, aligning with institutional size, maturity, and evolving operational needs.

SUCCESS STORY

Unifying Cybersecurity Across a Multi-Academy Trust with ESET PROTECT Complete

Managing cybersecurity across multiple school sites doesn't have to be complex. Discover how one UK multi-academy trust simplified its security operations, reduced IT overheads and gained full visibility and control by consolidating with ESET PROTECT Complete.

→ CUSTOMER

A multi-academy trust in the UK committed to raising education standards across its seven institutions at both primary and secondary levels. The trust emphasises high quality education through rigorous improvement strategies including consistent data monitoring and strategic, impactful, expansion.

→ WHY DID THEY COME TO ESET

The trust has been ESET partners for six years, and throughout that time has upgraded its solution to enable cloud and single interface usage across some of its academies. However, with multiple cybersecurity vendors covering their entire academy portfolio, they were running into integration issues, high maintenance overhead costs, and complex cybersecurity visibility and management.

→ HOW DID ESET PROVIDE A SOLUTION

With five locations, they struggled to find a single cybersecurity vendor that could cover all their requirements across the different sites. By upgrading to ESET PROTECT Complete, they migrated all their cybersecurity services to ESET. The trust now benefits from the ESET PROTECT management console providing a simple user interface to manage and operate their cybersecurity defences across the different sites with ease. The trust now has the capability to easily supply more locations and services as it grows with award-winning cybersecurity.

→ BEFORE

- Inconsistent security policies
- Higher costs
- Integration issues
- More IT resources are needed for management

→ NOW

- One single management interface for complete visibility and control
- Consistent security policies
- Seamless integration across sites
- Less IT overhead required

→ ESET PROTECT COMPLETE

- Complete multilayered protection for all endpoints, cloud applications, and email
- Mobile threat defence
- Full disk encryption
- Cloud app protection
- Vulnerability and patch management
- Server security

SUCCESS STORY

How a Hertfordshire Academy Transformed Protection and Productivity with ESET

Discover how a Hertfordshire secondary school transformed its cybersecurity strategy by switching to ESET PROTECT Complete, streamlining operations, reducing IT strain and enhancing protection across the board.

→ CUSTOMER

A secondary school academy in Hertfordshire established in 1964 with around 1,400 students.

→ WHY DID THEY COME TO ESET

The customer was originally using an ESET competitor for their cybersecurity solution, which they found to be 'clunky' and not efficient in what they needed it for.

→ HOW DID ESET PROVIDE A SOLUTION

Upon listening to the customer's pain points and cybersecurity requirements, we showcased our 365 security along with ESET endpoint protection. After learning about the features and the easy-to-manage unified control console, the customer decided to consolidate their entire cybersecurity services to just ESET. An extended trial of the ESET PROTECT Complete enabled them to switch over at the end of their budget cycle, whilst also giving them time to move everything to ESET prior placing the order.

→ BEFORE

- IT staff frustration and fatigue from inefficient management abilities
- Potential of higher error rates and increased vulnerabilities from a cumbersome interface
- Inefficient navigation and poor usability resulting in delayed threat detection and inaccurate monitoring

→ NOW

- Flexible deployment catering to their infrastructure and budget
- Dedicated support from ESET specialists
- A centralised remote management console for easy use and reduced operational complexity
- Multilayered security with robust endpoint protection
- Additional security features including cloud-based sandboxing and full disk encryption

→ ESET PROTECT COMPLETE

- Complete multilayered protection for all endpoints, cloud applications, and email
- Mobile threat defence
- Full disk encryption
- Cloud app protection
- Vulnerability and patch management
- Server security

Sources

- Censuswide ESET research
- Government stats