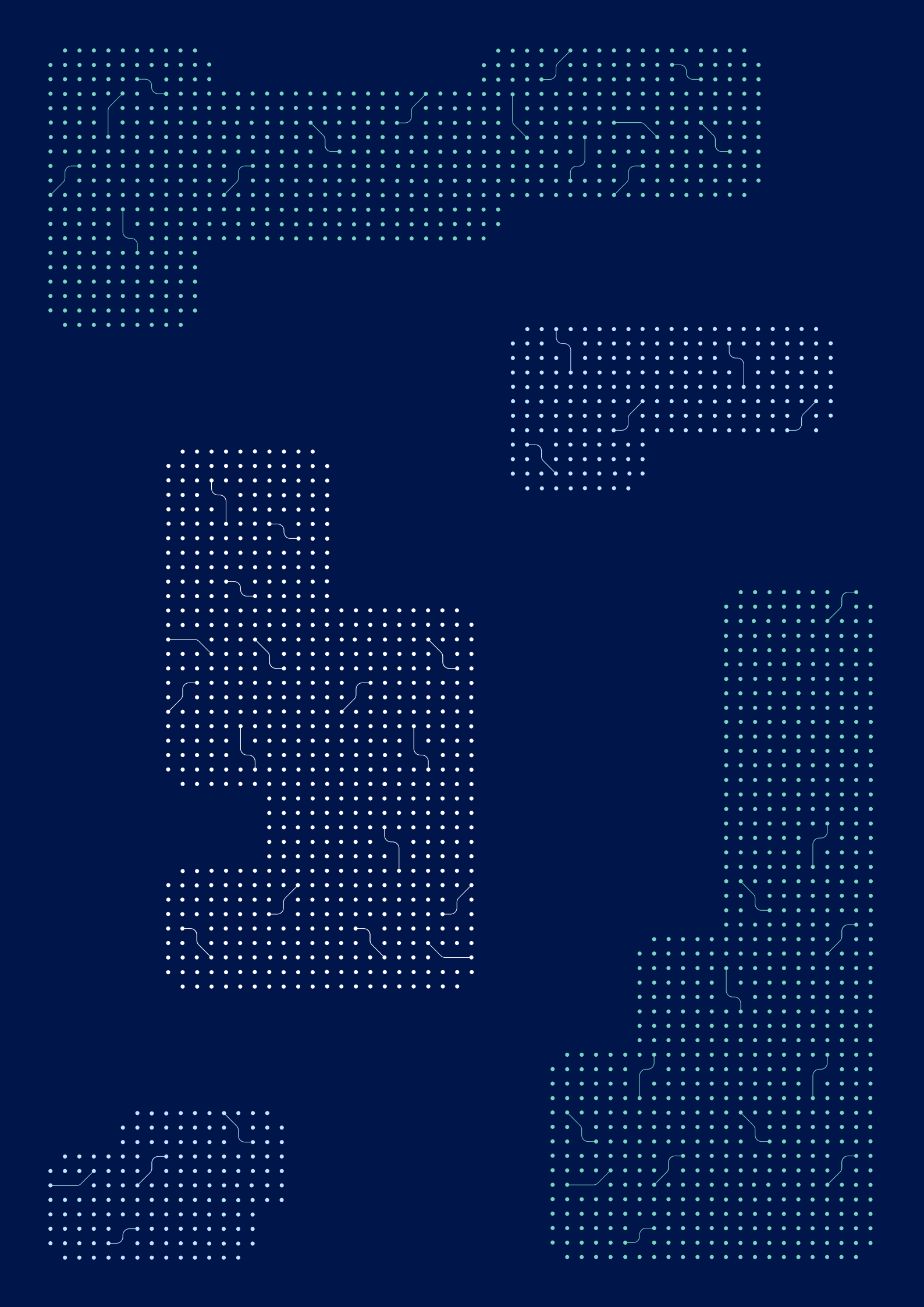
Secure Schools

The State of School Cybersecurity 2025



Why cybersecurity matters more than ever in 2025

Welcome to The State of School Cybersecurity report 2025

This State of School Cybersecurity report compiles key findings from extensive research with 600 schools and multi-academy trusts (MATs), specifically related to cybersecurity, safeguarding and digital best practice.

This year's research focuses on fundamental cybersecurity best practices, policies, and tools schools should use to match national government standards and put themselves in the strongest position to deter, mitigate, and limit the risks of a cybersecurity breach.

Our goal? To help schools reduce their cyber risks, protect learning, and track our collective progress over time. Let's get into it.

Methodology: *The data collected from cyber score participants identified which schools have confirmed the use of certain practices, tools and services. The responses and figures within this report do not explicitly state that schools are not taking these actions, simply that they have not confirmed them through their cyber score self-paced audit. The research is representative of approximately 600 schools that are considered 'engaged' with our cyber score tool.*

Key insights:

Cybersecurity is not just an IT issue, it's a whole school consideration:

- **Only 53% of schools** stated having a policy for password security.
- **Only 14% of schools** confirmed a dedicated person who has overall responsibility for cybersecurity.
- **Over half of schools or trusts** confirmed they delete/suspend staff accounts immediately after they leave the organisation.

Multi-factor authentication (MFA) is not yet widespread in schools

- **Only 46% of schools** stated the use of MFA on all available/ applicable devices, with 43% of schools confirming they have a policy related to staff using MFA.
- Additionally, **less than a quarter of schools** stated enabling MFA for cloud services to staff where supported.

Having a dedicated cyber incident response plan is critical:

- **Only 37% of surveyed schools** have stated they have a dedicated incident response plan.
- **In addition, less than half of schools** stated having sufficient backups on critical IT systems to operate for unplanned outages such as a cyber attack.

Schools require a greater understanding of their main vulnerabilities:

- **Less than 75% of schools or trusts** stated having regular vulnerability scans on their external IT infrastructure.
- **Just over a quarter of schools (27%)** stated conducting DPIA checks on third parties who process personal data.

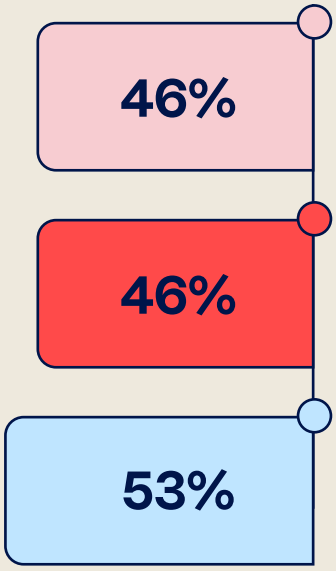
The main cybersecurity risks for schools

We've uncovered the most common cyber threats and vulnerabilities facing schools globally today. It's a snapshot of where the schools stand right now, and a starting point for anyone looking to strengthen their own cyber defences.

Account Compromise

With only 46% of schools reporting the use of multi-factor authentication (MFA) on all applicable IT team accounts, compromised credentials remain a high risk, particularly when accounts are not suspended promptly after staff departures.

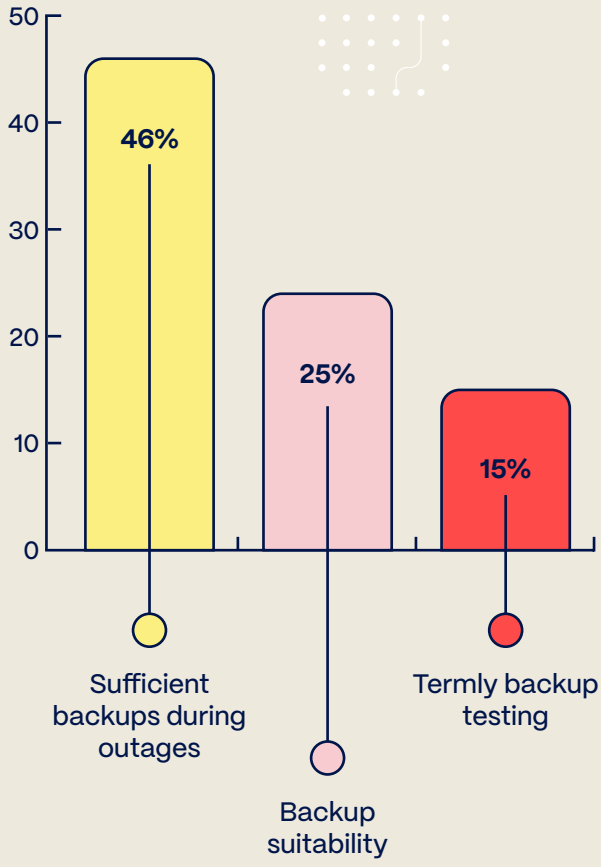
Schools remain highly vulnerable to credential compromise, one of the most common and costly cyber threats without robust account creation, suspension, and authentication controls.



Of schools stated they enforce MFA across all IT team accounts, leaving systems open to credential-based threats.

Stated new staff accounts are created before formal approval, posing a risk of unauthorised access.

Stated that staff accounts are always disabled or deleted promptly, increasing the potential for misuse.



Ransomware and Data Lockouts

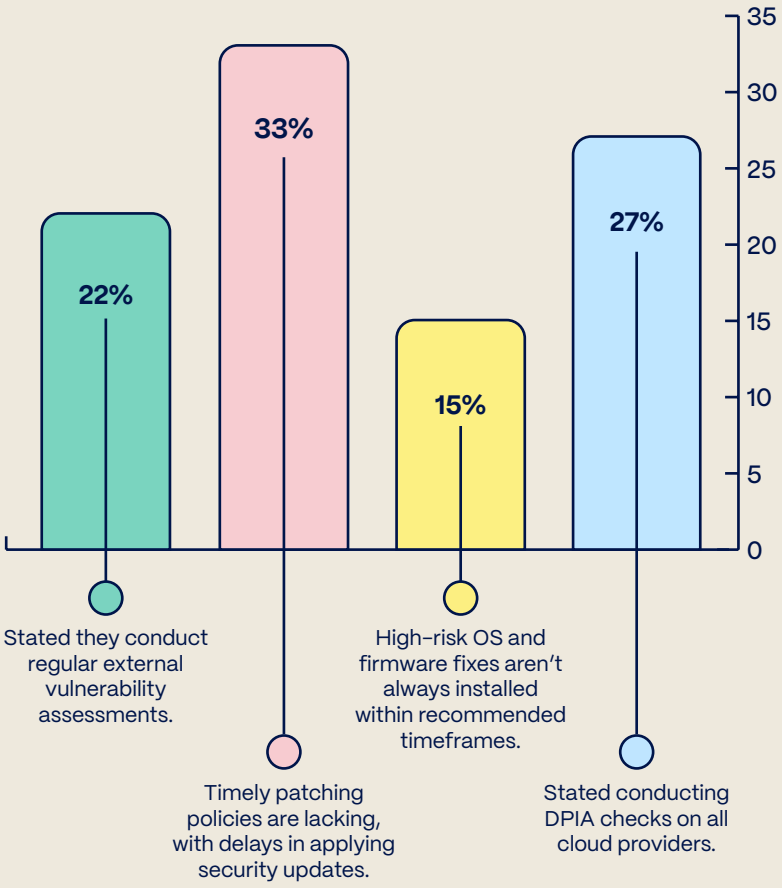
Only 46% of schools stated having sufficient backups to operate during unplanned outages. Any organisation, including schools, that fails to have appropriate backups leaves itself exposed during ransomware attacks.

A quarter of schools reported identifying suitable backup methods that meet operational needs.

Only 15% of schools stated conducting termly backup tests as part of disaster recovery exercises.

Unpatched Systems and Supply Chain Risk

Less than 75% of schools indicated conducting regular vulnerability scans, and just 27% stated conducting DPIA checks on vendors, highlighting widespread exposure through third-party tools and services.



50%
of schools have active password policies

<20%
have a dedicated cybersecurity lead

Policy Rollout and Compliance

Half of participating schools stated having active password policies, with less than 20% reporting a dedicated person whose overall responsibility within the school is cybersecurity.

Phishing Attacks

Email remains the primary route for cyber-attacks, yet many schools have not indicated that they conduct widespread staff training.

Email is #1 attack route

Training on **phishing threats** may not be widespread

What schools are doing well

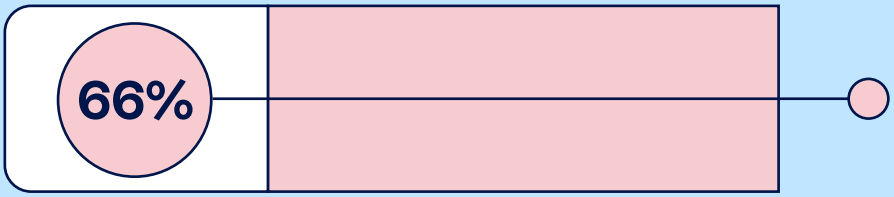
Despite the most common risks and pitfalls outlined in the previous section, schools and trusts are demonstrating strengths in several key areas of cybersecurity, with some of the most notable being:

- Email Security Fundamentals
- Password Policy
- Account Security

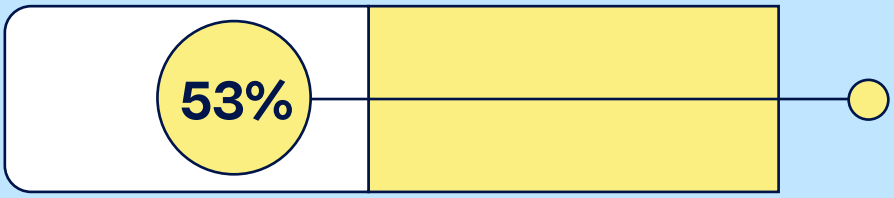
Email Security Fundamentals

A significant number of schools have implemented foundational email security measures.

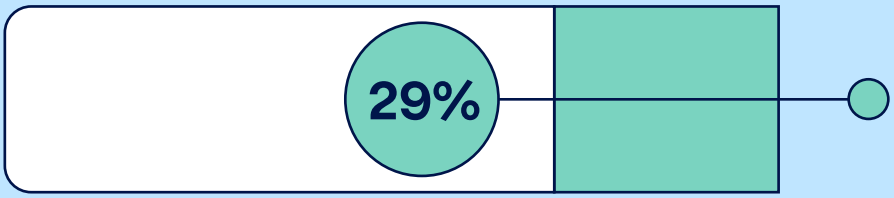
Foundational email security measures like Sender Policy Framework (SPF), Domain-based Message Authentication, Reporting, and Conformance (DMARC), and anti-malware scanning are gaining traction in schools, but broader adoption is still needed to close remaining gaps and strengthen protection against the most common type of cyber attack.



Schools stated **correctly implementing SPF records** for all owned domain names.



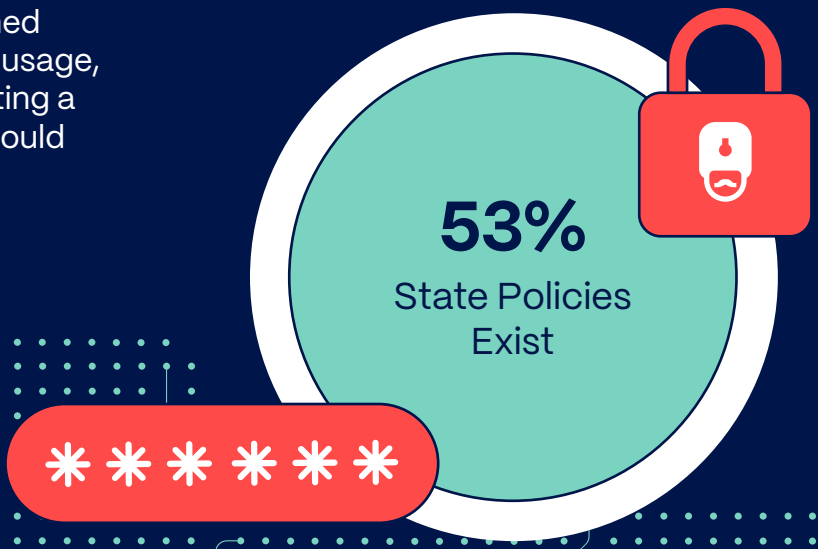
Schools that stated **having correctly implemented DMARC records** for all owned domain names.

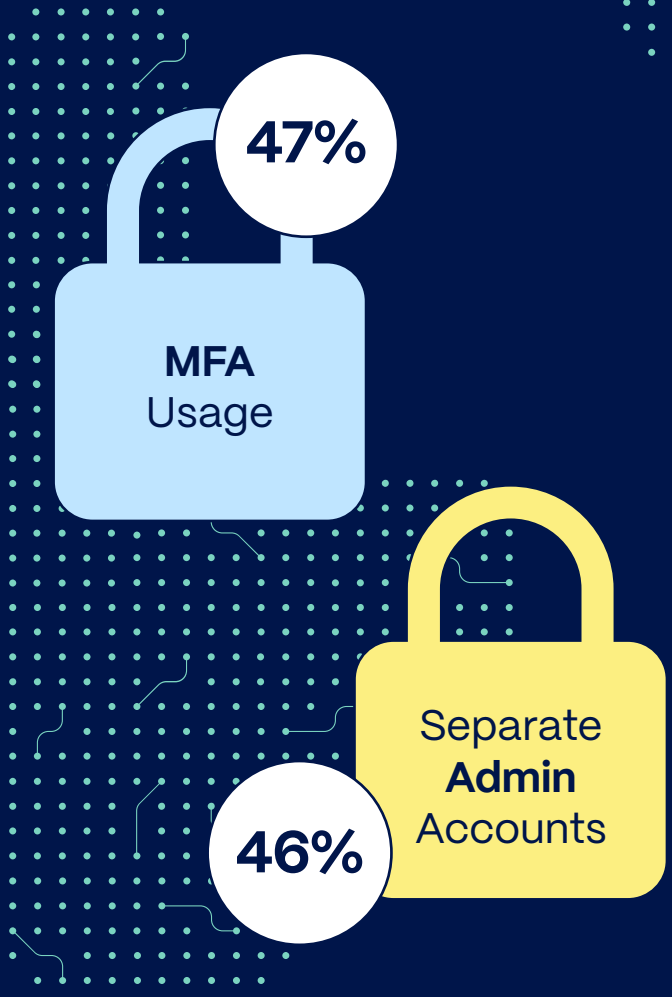


Schools stated **configuring locally installed anti-malware software** or a gateway anti-malware service to scan incoming and outgoing emails for malware.

Password Policy

Many schools have established policies regarding password usage, with over half of schools stating a policy detailing how users should use passwords.





Account Security

Despite being considered a potential area of improvement on the whole, our data found a notable focus on securing IT team accounts.

47% of schools stated their IT team uses multi-factor authentication on all of their accounts where it is available.

46% of schools stated their IT team has separate administrator accounts for maintenance and administrative activities.

The importance of incident response planning

Developing and implementing a robust incident response plan empowers schools to minimise the impact of potential cyber incidents and ensures continuity of learning.

While there's a clear opportunity for growth, our research highlights areas where schools can significantly strengthen their incident response capabilities.

Schools recognise the importance of early detection.

However, just one in ten schools stated having a mechanism for alerting relevant people when ransomware is detected, a crucial step in limiting damage.

Access to key information

Our data suggests that most incident response plans need more robust approaches to contact information and business continuity.

- Less than 15% of schools stated having contact details for the relevant department accessible during system unavailability.
- However, there's a rising understanding of the importance of comprehensive business continuity planning, with 15% of schools having a business continuity plan, more than other public sector industries have stated in other studies.

Back it up!

Schools are actively working towards more resilient backup strategies to safeguard operations against unplanned outages.

20%

Schools stated implementing the robust 3–2–1 backup strategy, the best practice for data protection in other 'high priority' target industries.

25%

Schools have stated having suitable backup methods that meet their operational needs.

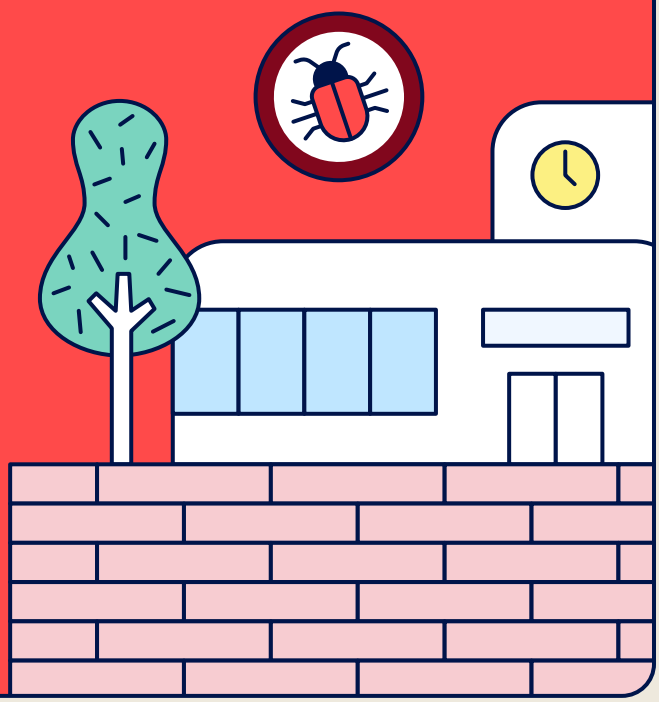
46%

Of schools are already ensuring their backups support continued operation during an unplanned event like a cyber attack.

Real-world evidence

In September 2024, the Fylde Coast Academy Trust in Lancashire suffered a ransomware attack affecting all ten schools under its umbrella, including both primary and secondary institutions, which rendered IT systems unusable; staff had to revert to non-digital processes for essential tasks like attendance, teaching, and communications, and recovery stretched into days or weeks.

This is just one example of hundreds that occur every year, and illustrates why schools must invest in robust, tested backup systems, not as optional admin overhead, but as mission-critical infrastructure to protect learning continuity, and data integrity.



How can schools reduce their cybersecurity risks?

Our findings highlight significant opportunities for schools and trusts to strengthen themselves against the most common cybersecurity threats.

So, what can schools do differently?

By building on existing strengths and addressing common vulnerabilities, schools can proactively mitigate risks and keep the focus on the most important aspect of their school – keeping education uninterrupted.

Based on cyber score data, here are the big-ticket, high-impact things schools can do to reduce their risks.

MFA widespread across devices and systems

While some progress has been made, widespread adoption of MFA across all applicable accounts is crucial. Getting this right reduces the risk of account compromise, even if passwords are stolen.

Current state: 43% of schools state having a policy for MFA usage; 24% state enabling MFA for all cloud service users.

Aspiration: Aim for universal MFA implementation across all staff and cloud services where supported.

How to get there:

- **Develop and enforce** a clear, mandatory MFA policy for all users and services.
- **Provide comprehensive training** and support to staff on enabling and using MFA.
- **Prioritise MFA** rollout for high-risk accounts, such as IT administrators and leadership.

You can print out these pages, and use the tickboxes to track progress and reduce cybersecurity risks.

Proactive, regular vulnerability management and patching

Regular vulnerability assessments and timely patching are key layers of cybersecurity defences. A proactive approach to identifying and addressing system weaknesses minimises exposure to known exploits and usually mitigates the 'hot topic' ways hackers look to exploit your systems.

Current state: 22% of schools state conducting regular external vulnerability assessments one in three state having a policy to install patches within 14 days. A quarter state installing critical OS/ firmware fixes within 14 days.

Aspiration: Establish a continuous and rigorous vulnerability management program with prompt patching cycles.

How to get there:

- **Dedicate resources** for both internal and external infrastructure scans and audits.
- **Develop a clear patch management strategy, prioritising critical updates.**
- **Regularly review and update** hardware and software to ensure they remain supported by vendors.

Improved Third-Party/ Supply Chain Risk Management

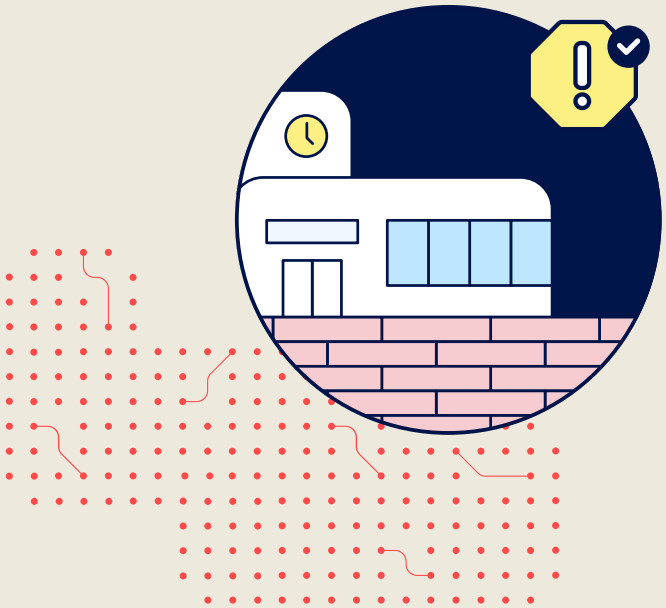
The interconnected nature of digital services means that a school's cybersecurity is only as strong as its weakest link, often found within its supply chain. Robust due diligence on third-party vendors is absolutely paramount.

Current state: 28% of schools state that they are completing Data Processing Impact Assessments (DPIAs) for cloud suppliers.

Aspiration: Implement a comprehensive third-party risk management framework, ensuring suppliers adhere to stringent cybersecurity standards.

How to get there:

- **Conduct thorough** security assessments and DPIAs for all new and existing cloud and IT service providers.
- **Integrate data security** requirements into all supplier contracts.
- **Regularly review** supplier cybersecurity compliance.



Plan, mitigate, communicate...

An untested plan is an unreliable plan. Developing a detailed cybersecurity incident response plan and regularly testing it means your school can respond effectively and minimise disruption during a cyber incident.

Current state: 38% of schools stated having a dedicated incident response plan.

Aspiration: Establish a well-documented, regularly tested, and clearly communicated incident response plan.

How to get there:

- **Develop a comprehensive** incident response plan, including roles, responsibilities, communication protocols, and recovery procedures.
- **Conduct annual tabletop exercises** or simulated incident drills to test the plan's effectiveness.
- **Keep all relevant staff trained** and diligent on their roles within the incident response framework.
- **Maintain easily accessible contact details** for key external support (e.g., education department, cyber resilience centres) in case of system outages.

Create a culture of cybersecurity accountability

Cybersecurity is not just an 'IT problem', it's a shared responsibility across the school. Embedding it into governance structures and assigning clear ownership at a senior level will drive consistent implementation and elevate its strategic importance.

Current state: Only 15% of schools stated having a designated cybersecurity lead, with 10% of schools stating that senior leadership and governors regularly discuss cybersecurity in their governance meeting.

You can print out these pages, and use the tickboxes to track progress and reduce cybersecurity risks.

Aspiration: Foster a whole-school approach where cybersecurity is a core governance priority with clear senior leadership oversight.

How to get there:

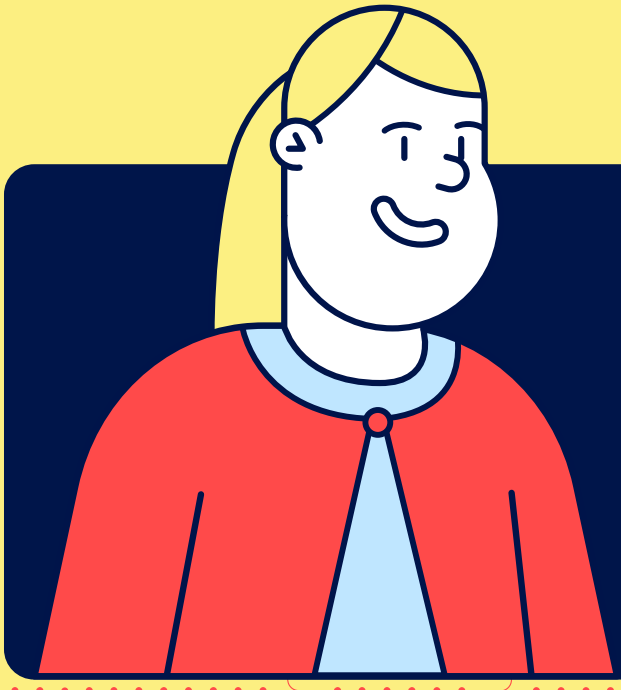
- **Appoint a senior leader** with explicit responsibility for cybersecurity strategy and oversight, which the DfE are already mandating for academy trusts.
- **Regularly include cybersecurity** on the agenda for governance meetings (e.g., audit and risk committees).
- **Provide cybersecurity awareness** training tailored to different staff roles, from administrative staff to board members.
- **Develop and communicate** clear acceptable use and password policies, ensuring staff understand their roles in maintaining security.

Conclusion

The State of School Cybersecurity report will be an annual study designed to illuminate the biggest risks in schools and highlight the great work we are doing as a collective to reduce them.

As the years go on, we hope this report will be an annual success story, showing the year-over-year upward trends of more schools globally, adopting best practices, following the recommendations of cybersecurity experts. Not just from us, but from the governing standards, and other fantastic companies all working towards the common, collective goal of reducing the risks cybersecurity poses to our education system.

While some of these stats are alarming, this report is not designed to spark fear. Cybersecurity best practice is built in stages, and each action you take, big or small, creates another layer of defence for your school. Every action you take, policy you implement, or initiative you launch to reduce risks will have an impact if you follow the right steps.



The best way to start tracking where your school is on its cybersecurity journey is through **Secure Schools' cyber score**.

It's a completely free resource that gives you a self-paced and easy way to benchmark your cybersecurity, identify key improvements, and better protect your school from cyber attacks.

No cost, no catch! Get started

Cyber score
by Secure Schools

Try Secure Schools Foundations for free

Measure and improve your cyber defences using our easy-to-use cyber score, available in **Secure Schools Foundations**!

Get started for free

Secure Schools

secureschools.com

hello@secureschools.com

Book time with our experts