Action1

Action1 Cybersecurity in Education Report 2025–2026

Table of contents

Introduction

Action1 surveyed more than 350 school IT leaders and administrators worldwide to assess how schools are managing cybersecurity risks midway through the 2025–2026 academic year and the challenges they face as they move into 2026. Now in its second consecutive year, this study builds on our 2024 findings and provides a year-over-year view of how school cybersecurity programs are evolving under growing operational and threat pressure (see our 2024 School Cybersecurity Survey blog for last year's findings).

The research examines how security maturity is progressing, where critical weaknesses remain, and which threats and structural barriers are shaping schools' risk exposure today. It explores cybersecurity preparedness, budget and staffing realities, real-world incident experience, and the adoption of key protective measures such as vulnerability assessments, phishing training, and multi-factor authentication.

Together, these insights offer a real-time snapshot of how schools are responding to today's cyber threats, while also highlighting where critical gaps may continue to challenge their ability to keep pace with an increasingly sophisticated threat landscape through 2026.

Executive Summary

1. Schools are reassessing their cybersecurity readiness more realistically.

Most school IT leaders now rate their cybersecurity maturity as moderate (66%), while confidence in being highly prepared has declined (18%, down from 30% in 2024), reflecting a clearer understanding of today's increasingly complex threat landscape.

2. Cyber incidents are now the norm, not the exception, in schools.

Over 85% of schools experienced at least one cyber incident in the past year, most commonly phishing, unauthorized access, and malware, with a subset resulting in data exposure (14%), learning disruption (11%), financial loss (9%), or reputational impact (95).

3. Cybersecurity investment is rising, but chronic staffing shortages continue to limit its impact.

While more schools report stable or rising security budgets, nearly 40% still feel under-protected against ransomware, and almost three-quarters operate without a dedicated cybersecurity specialist, limiting the effectiveness of these investments.

4. The biggest barriers to stronger cybersecurity are structural, not technical.

Budget limitations, legacy infrastructure, staffing shortages, and low cybersecurity awareness among users continue to slow security improvements and directly align with the attack methods schools fear most, including phishing and credential theft.

5. Schools are improving proactive security practices — but unevenly.

More schools now conduct regular vulnerability assessments, signaling progress toward proactive risk management, yet phishing simulations remain inconsistent despite phishing being the most prevalent attack vector.

6. AI-driven phishing and ransomware dominate schools' forward-looking risk concerns

An overwhelming majority of school IT leaders (92%) expect AI-powered phishing to be the most dangerous threat in the coming year, surpassing ransomware, which remains a significant risk. Account takeovers and attacks on sensitive student and staff data also rank among the most serious anticipated threats.

Present-Day Cybersecurity Maturity Among Schools

We asked school IT leaders and administrators to assess their overall cybersecurity posture for the 2025–2026 academic year. Respondents overwhelmingly place their schools in the “Moderately Prepared” range (66%), marking a notable shift upward from last year (54%). Only 18% feel “Very Prepared,” a significant drop from 30% in 2024, while “Slightly Prepared” remains largely unchanged at 16%. No respondents rated their schools as entirely unprepared, suggesting that most institutions perceive at least a foundational level of security.

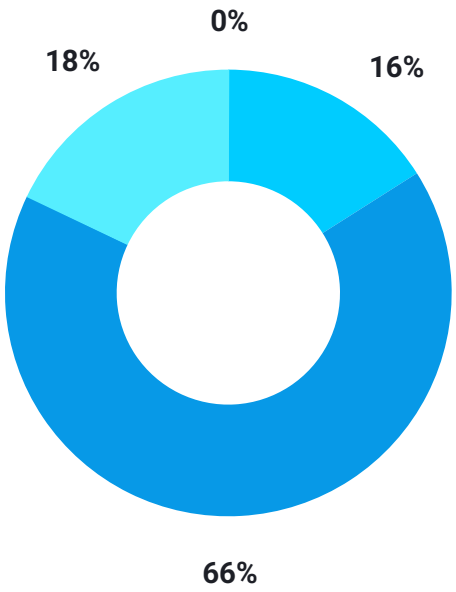


Chart 1.

How would you rate your school‘s overall cybersecurity posture for the 2025-2026 academic year?

- Not Prepared at All
- Slightly Prepared
- Moderately Prepared
- Very Prepared

Schools are now far more likely to place themselves in the mid-range of preparedness, with a significant shift away from the highest readiness tier. This doesn’t point to declining security, but rather to heightened awareness and more realistic standards in light of today’s expanding threat landscape.

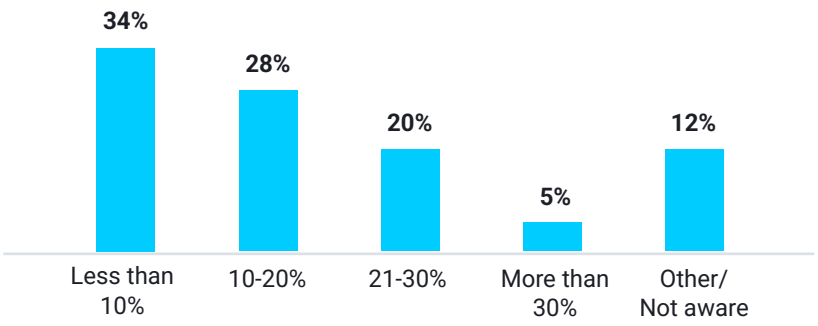
School Cybersecurity Funding Trends

This year, most schools still dedicate a relatively small portion of their IT budget to cybersecurity, but the distribution is moving in a positive direction. The share of organizations spending less than 20% of their IT budget dropped from 81% in 2024 to 62% in 2025. Meanwhile, those allocating 21–30% increased sharply from 5% to 20%, and the proportion spending more than 30% rose from 2% to 5%.

Spending is gradually increasing, with fewer schools in the lowest budget brackets and more allocating mid- to higher-range funds. This shift indicates growing recognition of the financial demands of modern cybersecurity, even as overall investment still lags behind the threat realities for many educational organizations.

Chart 2.

What percentage of your IT budget is allocated to cybersecurity?



Half of the respondents report that their cybersecurity budget remained stable this year, while more than one-third saw an increase. Only 9% experienced a decrease, suggesting that cuts in this area are relatively uncommon.

The data indicates that cybersecurity spending is generally holding steady or trending upward despite broader financial pressures. This pattern aligns with the gradual increase in allocation percentages shown in Chart 2.

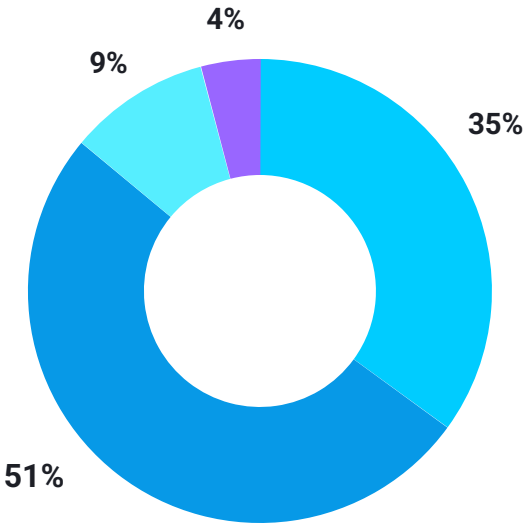


Chart 3.

Compared to previous years, how has your school's cybersecurity budget changed this academic year?

Schools are beginning to invest more seriously in cybersecurity, with mid-range budgets rising sharply year over year.

Many schools report either stable or increased cybersecurity funding, reflecting recognition of the growing risks facing the education sector. Overall, the data suggests that maintaining and strengthening cyber defenses is becoming a higher priority for school IT leadership.

Resource Constraints Amid Growing Threats

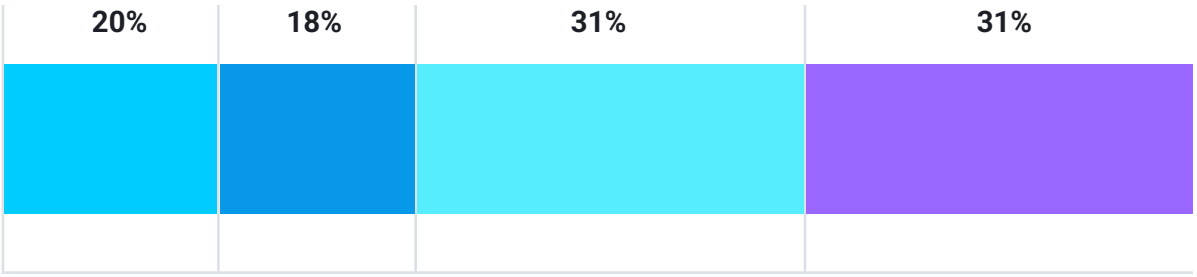
Following up on last year's finding, in which over 60% of school IT leaders warned that ransomware threatened education quality, we surveyed schools to estimate the support they receive for ransomware prevention in the 2025-2026 academic year.

This year, responses are more nuanced: about 62% of schools feel that their current support for ransomware prevention is sufficient, though half of these still express some concern about potential disruption. The remaining 38% indicate that support is insufficient, with varying degrees of perceived risk to learning, research, or operations.

Overall, approximately half of surveyed IT leaders (51%) view ransomware as a continuing threat to the education process.

Chart 4.

Do you believe your school currently receives sufficient support for ransomware prevention to avoid significant disruption to learning, research, or operations in the event of a successful attack?



- No, the current support is insufficient, and the risk of a significant impact on education quality is high.
- No, the current support is insufficient, but the risk of a significant impact on education quality is moderate.
- Yes, the current support is sufficient, and the risk of a significant impact on education quality is low.
- Yes, the current support is sufficient, but the risk of a significant impact on education quality is still a concern.

These results suggest that while many schools are investing more in cybersecurity (as seen in Chart 2 and Chart 3), gaps in confidence and perceived effectiveness remain—even among institutions allocating significant resources.

Nearly 40% of schools still feel under-supported, highlighting that financial investment alone is not enough; proper tools, policies, and expertise are essential to effectively reduce ransomware risk.

In addition, the survey found that cybersecurity roles remain critically understaffed in education, with 74% of schools still lacking a dedicated specialist—a pattern that appears nearly unchanged from last year.

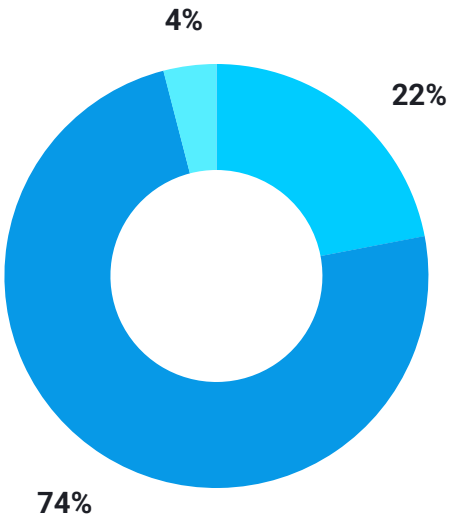


Chart 5.

Do you have a dedicated cybersecurity specialist in your team?

- Yes
- No
- Other

Despite growing investment in cybersecurity and increasing awareness of ransomware risks (as seen in earlier questions), schools continue to face significant talent and staffing constraints. The lack of specialized personnel limits their ability to implement, tune, and continuously maintain security controls, suggesting that budget increases alone have not translated into expanded security teams.

Current Threat Landscape and Security Practices in Schools

Cyber Incidents and Their Impact in Schools

Most schools (89%) reported experiencing at least one cyber incident in the past 12 months, with phishing as the dominant issue. While high-impact events like ransomware remained relatively rare, other forms of compromise (such as unauthorized access and malware) persisted across many environments.

Most commonly reported incidents:

Phishing attacks:

84%

Unauthorized access / account compromise:

22%

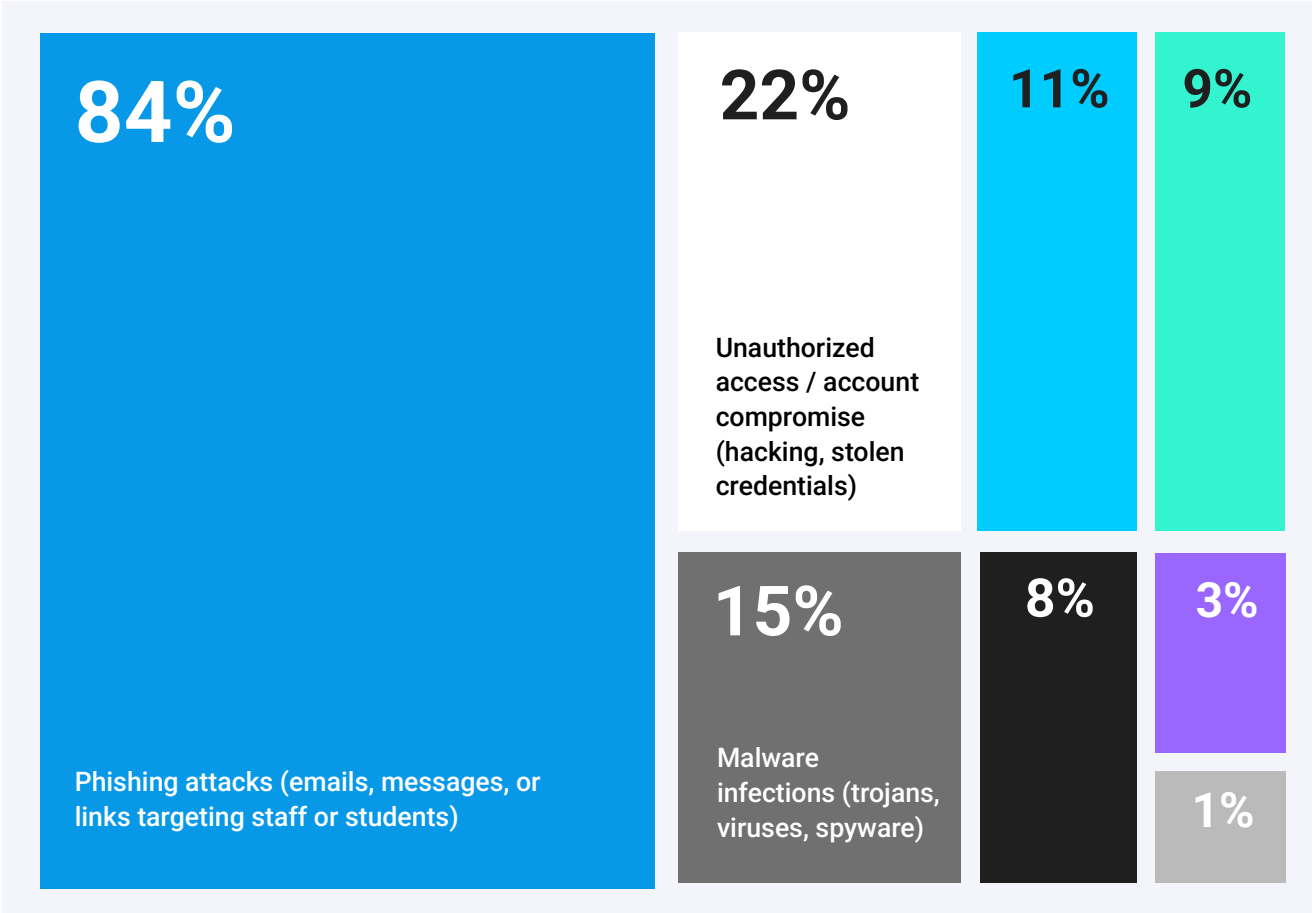
Malware infections:

15%

Only a small proportion encountered ransomware (3%), and only about one in ten schools reported no cyber incidents at all, highlighting wide variation in exposure across institutions.

Chart 6.

Have you experienced any cyber incidents in the past 12 months?



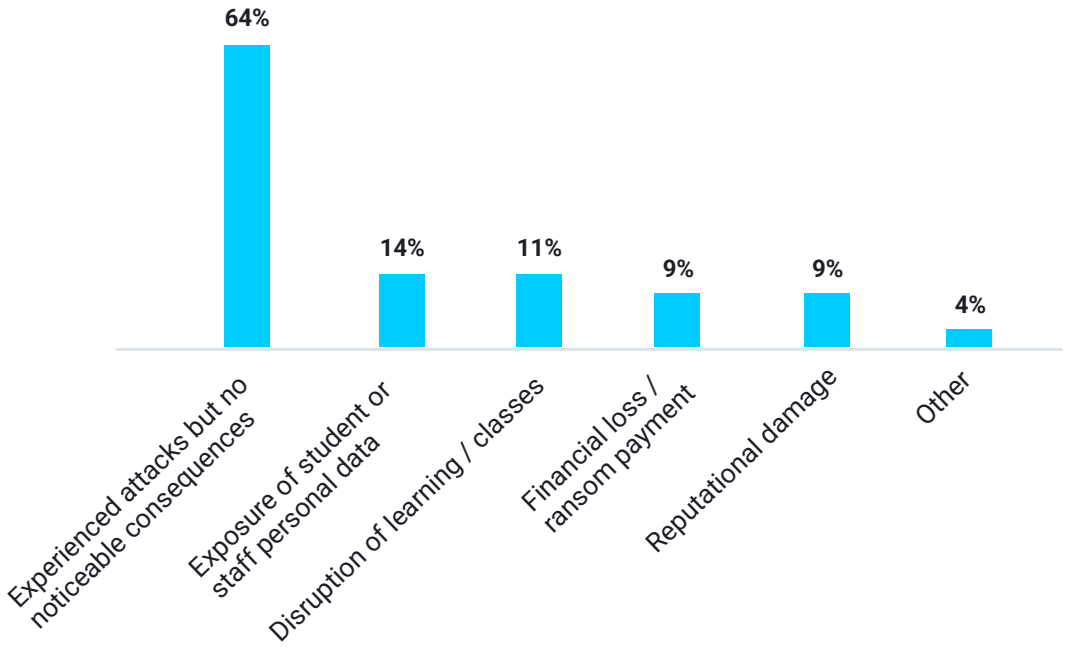
Nearly 9 in 10 schools were hit by cyber incidents in the past 12 months, driven largely by phishing, with fewer attacks leading to serious disruption.

We also surveyed school IT professionals about the consequences their institutions experienced due to cyber incidents. Nearly **two-thirds of schools** indicated that attacks occurred but **did not result in noticeable consequences.**

When incidents did have tangible effects, the most common outcomes involved exposure of personal data (14%), disruption to learning (11%), financial losses (9%), and reputational damage (9%).

Chart 7.

Which of the following consequences did your school experience due to these incidents?



Together, these findings highlight a dual reality: **schools face frequent, persistent threats**, yet many are **partially resilient** or able to mitigate impacts. Nevertheless, the presence of high-risk incidents, even if infrequent, underscores the ongoing need for proactive security practices and robust incident response.

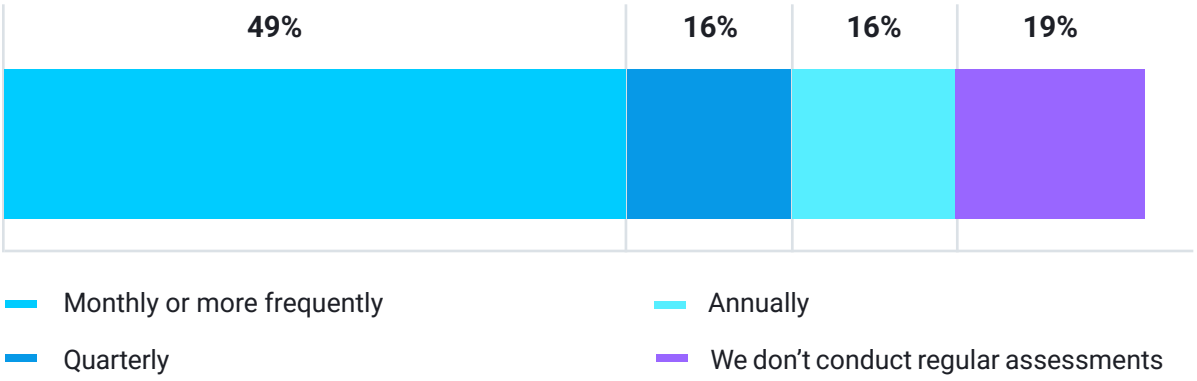
Proactive Cybersecurity Measures

Vulnerability Assessments

Schools are increasingly performing regular vulnerability assessments, with many now checking endpoints monthly or more often (49%, up from 27% in 2024). Less frequent or irregular assessments are becoming less common, indicating a stronger focus on consistent risk management.

Chart 8.

How often do you conduct vulnerability assessments on your endpoints?



Phishing Emulation Tests

Schools vary widely in how often they conduct phishing emulation tests, which help teachers recognize and respond to malicious links. While some institutions test monthly or more frequently (19%, up from 11% in 2024), a third run them quarterly (34%, slightly down from 39% in 2024), and a significant portion still conducts tests only once a year, or not at all (36%).

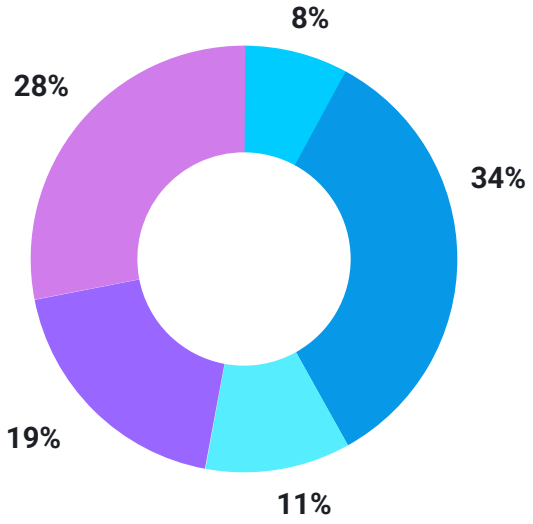


Chart 9.

How often do you conduct phishing emulation tests to ensure that teachers are aware of how to identify malicious links?

- We did it once
- Quarterly
- Annually
- Monthly or more frequently
- We don't conduct phishing emulation

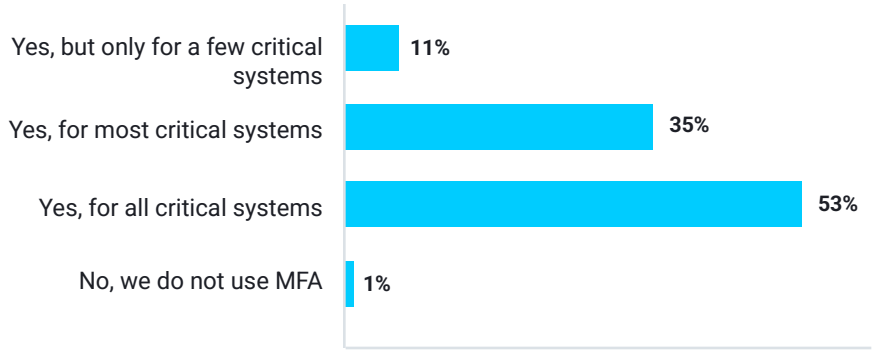
Multi-Factor Authentication (MFA) Use

Most schools now implement MFA for their critical systems, reflecting growing adoption of this essential security control. Over half of institutions (53%, up from 44% in 2024) use MFA for all critical systems, while a sizable portion applies it to most systems (35%, down from 46% in 2024). A smaller group uses MFA only for a few systems (11%, up from 7% in 2024), and very few schools still do not use MFA at all (1%, down from 3% in 2024).

Approximately every fifth teacher is not fully compliant with MFA, a proportion that remains similar to last year.

Chart 10.

Do you use Multi-Factor Authentication (MFA) for critical systems?



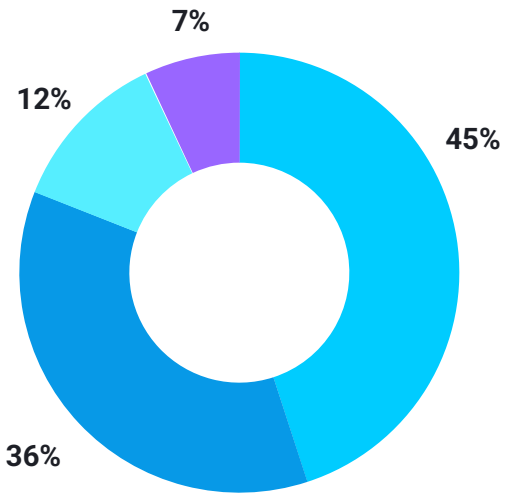


Chart 11.

How compliant are teachers in following MFA guidelines?

- Very compliant
- Moderately compliant
- Slightly compliant
- Not compliant at all, they are rather reluctant to use it

Future Risks and Barriers

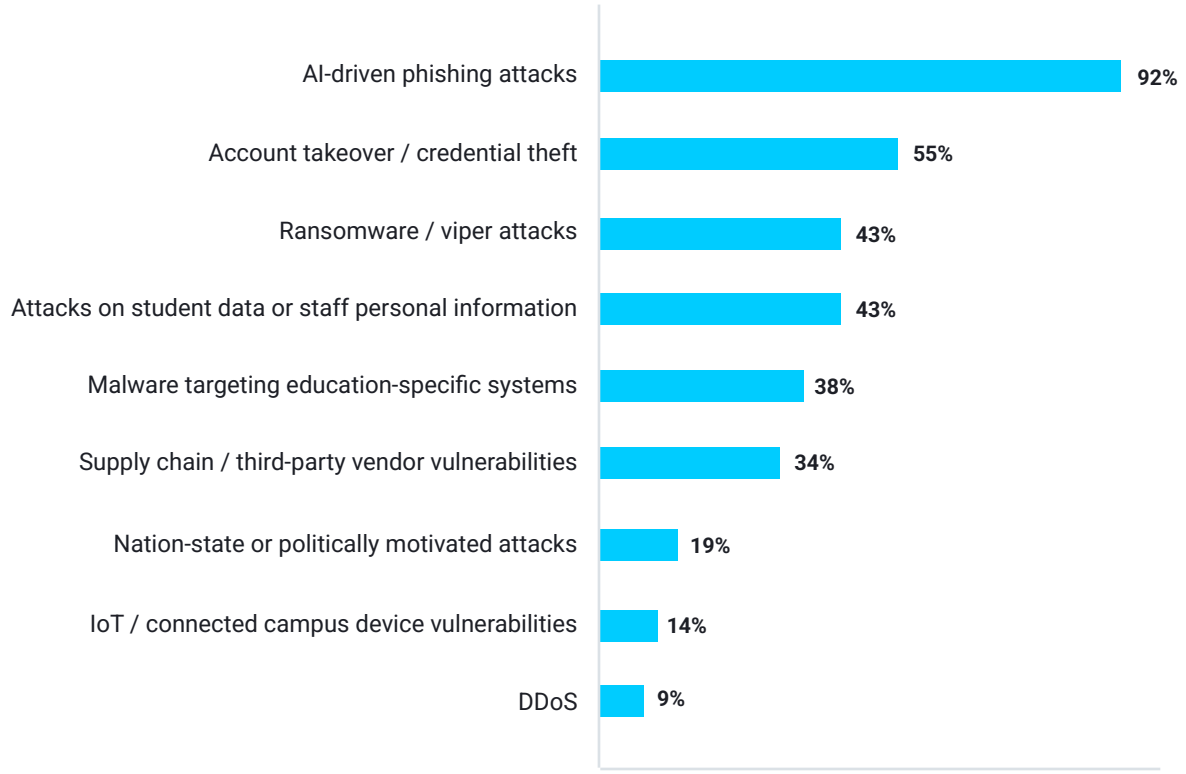
Emerging Cyber Threats Poised to Impact Schools

School IT leaders are increasingly concerned about sophisticated cyber threats in the coming year, with AI-driven phishing seen as the top risk by an overwhelming majority (92%). Ransomware (43%), account takeovers (55%), and attacks on sensitive student or staff data (43%) are also prominent concerns.

While less common threats, such as nation-state attacks (19%), DDoS (9%), or IoT vulnerabilities (14%), are noted, the focus clearly lies on social engineering, credential compromise, and malware targeting education systems.

Chart 12.

What emerging cybersecurity threats do you expect to impact your school the most in the next year?



Barriers to Strengthening School Cybersecurity

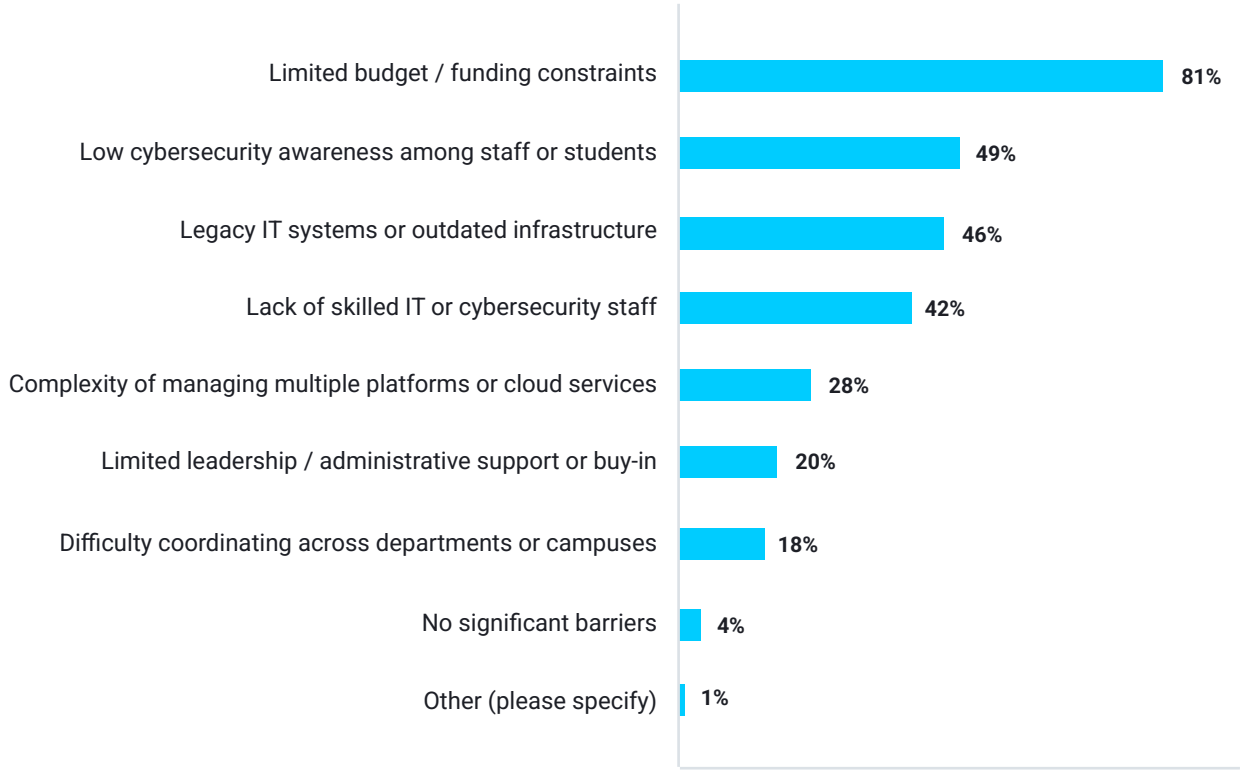
Even as cyber risks escalate, school IT leaders face persistent structural barriers that limit how quickly and effectively they can strengthen security, shaping nearly every cybersecurity decision and slowing progress across the sector.

Key challenges identified:

- **Limited budget / funding constraints (81%)** — by far the most common barrier, shaping every other security decision and slowing modernization efforts.
- **Low cybersecurity awareness among staff or students (49%)** — nearly half struggle with human-factor risks that expose schools to phishing, credential theft, and social engineering.
- **Legacy IT systems or outdated infrastructure (46%)** — older systems introduce exploitable weaknesses and complicate integration with modern defenses.
- **Lack of skilled IT or cybersecurity staff (42%)** — ongoing staffing shortages limit the ability to manage and respond to threats effectively.

Chart 13.

What are your biggest barriers to improving cybersecurity at your school?



Together, these results highlight a critical tension between rising cyber risks and the practical limits of school cybersecurity readiness.

- **Attack sophistication is now outpacing school defenses,** as cyber techniques are evolving faster than most schools can adapt their security programs.
- **The most feared threats directly exploit schools' weakest points,** with AI-enhanced phishing and credential-based attacks targeting limited budgets, human-factor risks, and outdated infrastructure.
- **Structural constraints are slowing schools' ability to respond:** funding limitations, staffing shortages, and legacy systems restrict how quickly defenses can modernize despite growing risk awareness.

Recommendations

1. Strengthen Endpoint Protection and Monitoring

Deploy a comprehensive endpoint protection solution that can detect suspicious activity, prevent malware, and respond to incidents quickly. This is particularly important given the limited availability of cybersecurity staff and the prevalence of phishing, credential theft, and ransomware threats.

2. Leverage Automated Patch Management

Use automated tools to keep operating systems, applications, and endpoints up-to-date. Automated patching reduces the manual workload on IT teams, closes critical security gaps, and mitigates the risk of ransomware or malware exploiting outdated systems.

3. Implement Regular Vulnerability Assessments

Conduct monthly scans on all endpoints and key systems. Prioritizing consistent assessments helps identify weaknesses before they are exploited and aligns with proactive risk management practices highlighted in the survey.

4. Strengthen Identity Security Through MFA and User Awareness

Enforce multi-factor authentication across all critical systems and address compliance gaps proactively. Pair this with regular phishing simulations and targeted cybersecurity training for staff and students to reduce human-factor risks and credential-based attacks.

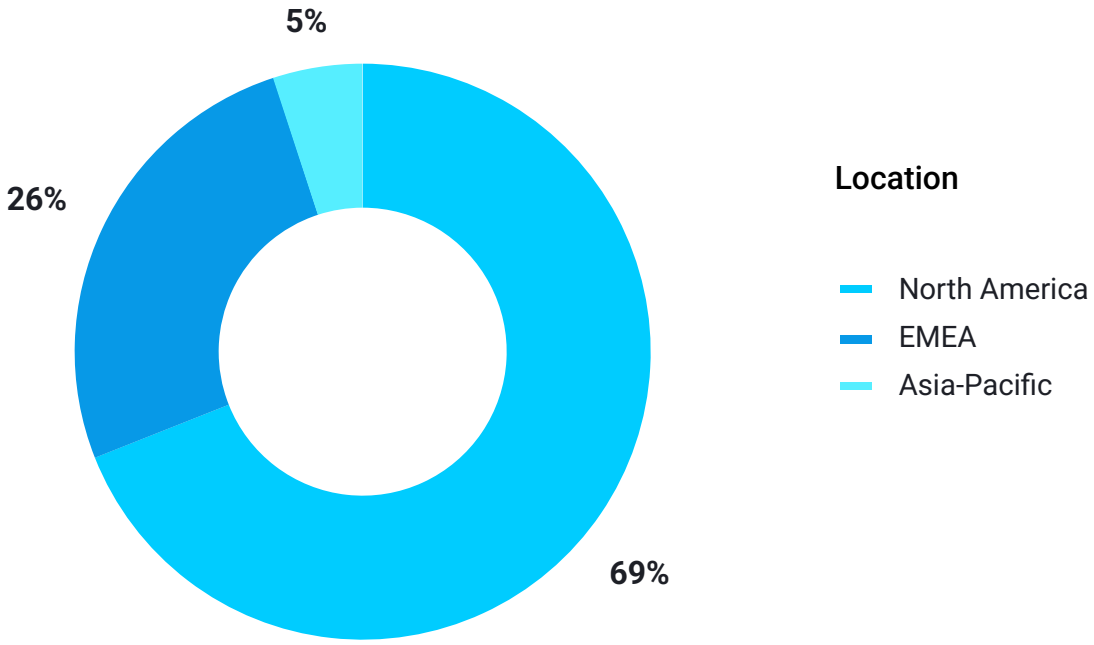
5. Adopt a Risk-Based, Zero-Trust Mindset

Operate under the assumption that any device, account, or user could be compromised. Implement strict access controls, network segmentation, and verification for every access request to limit the impact of potential breaches.

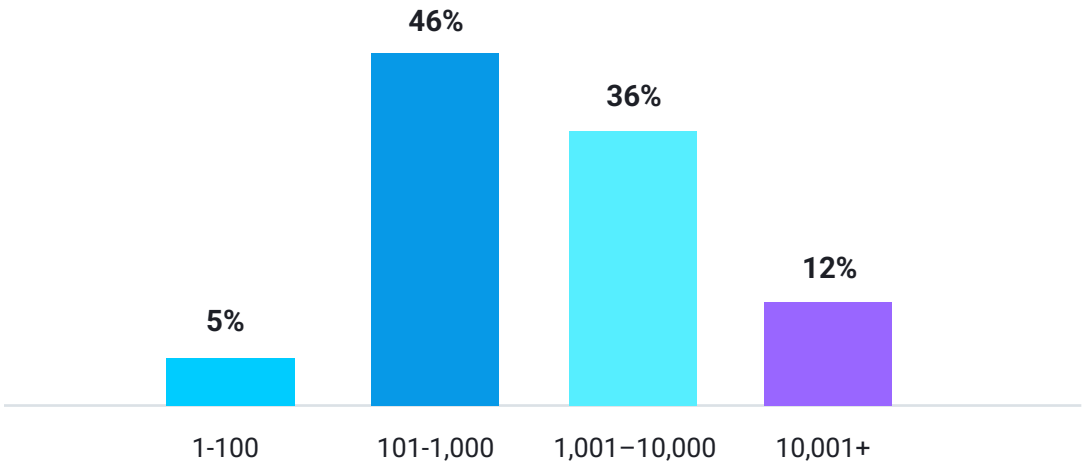
6. Plan for Incident Response and Disaster Recovery

Develop and regularly test disaster recovery and backup procedures to minimize disruption from cyber incidents. Ensure that recovery plans cover student data, learning continuity, and critical operations to mitigate the impact of ransomware or other attacks.

Survey Respondent Profile



IT Environment Size (by Endpoints)



Action1 Cybersecurity in Education Report 2025–2026

The report is brought to you by Action1 Research, which conducts industry surveys of cybersecurity practitioners worldwide to identify cybersecurity trends. For more information, please visit:

www.action1.com/resources/research/

About Action1

Action1 is an autonomous endpoint management platform trusted by many Fortune 500 companies. Cloud-native, infinitely scalable, highly secure, and configurable in 5 minutes—it just works and is always free for the first 200 endpoints, with no functional limits. By pioneering autonomous OS and third-party patching with peer-to-peer patch distribution and real-time vulnerability assessment without needing a VPN, it eliminates routine labor, preempts ransomware and security risks, and protects the digital employee experience.

In 2025, Action1 was recognized by Inc. 5000 as the fastest-growing private software company in America. The company is founder-led by Alex Vovk and Mike Walters, American entrepreneurs who previously founded Netwrix, a multi-billion-dollar cybersecurity company.

Learn more at: www.action1.com

Patch Management for Education
action1.com/education

Customer Stories
action1.com/case-studies/

Watch Demo
action1.com/watch-demo

© 2025 Action1 Corporation. All rights reserved.

Use of this document is subject to the Terms of Use.