CIS Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Contact
www.cisecurity.org
learn@cisecurity.org
518-266-3460

Protecting our Schools: Insights from the 2025 CIS MS-ISAC K-12 Cybersecurity Report

Addressing the multi-layered threat to schools

Introduction

Imagine a high school during midterms: students focused on exams, teachers grading assignments, and cafeteria staff preparing meals. Suddenly, everything grinds to a halt—no access to online tests, meal payment systems frozen, and parents scrambling to find childcare as classes are cancelled. This isn't a hypothetical scenario; it's a reality many schools face due to cyber attacks.

The Alarming Statistics

More than 5,000 K-12 institutions were studied over 18 months (July 2023 through December 2024), and the findings are eye-opening:

82%
of reporting K-12 schools experienced cyber threat impacts

14,000
Nearly 14,000 security events were observed

9,300
More than 9,300 confirmed cyber incidents occurred

These numbers demonstrate that schools are prime targets for cybercriminals, and the consequences extend beyond data loss. Attacks disrupt meals, force closures, and prevent students from accessing crucial services like special education and counseling.

Understanding the Threats

Schools provide a unique range of services—education, meal programs, safe spaces, extracurriculars and social services. Cybercriminals exploit this dependency, knowing that disruptions will cause chaos and force quick responses.

The 2025 CIS MS-ISAC K-12 Cybersecurity Report explores how schools are tackling cyber threats through collaboration, preparation, and a people-first approach.

It emphasizes that cybersecurity in education is about safeguarding students, teachers, and communities—not just technology.

In this brief we'll provide the highlights of that report and explain how schools can strengthen their defenses and stay ahead of evolving threats.

Cybersecurity in education is about safeguarding students, teachers, and communities—not just technology.

The top threats schools face include:

RANSOMWARE ATTACKS

Malicious software locks school systems, demanding payment to regain access. These attacks often peak during critical periods like exams.

PHISHING AND SOCIAL ENGINEERING

Cybercriminals trick staff into revealing login credentials by posing as trusted sources.

MALVERTISEMENT

Malicious software, often disguised in seemingly harmless ads, infiltrates school networks and steals information.

DATA BREACHES

Sensitive student and staff data is stolen, leading to identity theft or leaks of personal information.

Unlike corporations with dedicated information security teams, schools often lack adequate funding and expertise. Additionally, school environments promote collaboration and openness, making it easier for cybercriminals to exploit human trust.

DENIAL-OF-SERVICE (DOS) ATTACKS

Cybercriminals overwhelm school networks, making online resources inaccessible.

The study found that cybercriminals are:

Shifting their focus, increasing attacks on the human element.
(e.g., phishing and social engineering) at least 45% rather than exploiting technical weaknesses.

Targeting critical academic periods, such as exam weeks, to maximize disruption.

Exploiting staff and students' reliance on digital tools.

Collaborating for a Safer Future

Cybersecurity is more than an IT issue—it's a community-wide effort. The report highlights that schools with partnerships in place recover faster and experience less disruption.

By working with MS-ISAC, schools gain access to:

- No-cost incident response services to handle cyber threats.
- Threat intelligence sharing to stay ahead of emerging dangers.
- Cybersecurity frameworks to strengthen defenses, enabling cybersecurity budgets to go further.

MS-ISAC®

Additionally, working with local government agencies, technology providers, and community organizations can help schools protect students, teachers, and families from cyber disruptions.

Cybersecurity is Community Security

The evolving threat landscape makes it clear: cybersecurity is essential for K-12 organizations of all sizes. Cyber attacks on K-12 institutions disrupt learning, compromise sensitive data, and place undue stress on educators, students, and families. However, with the right strategies in place, schools can build resilience against these threats. Schools that prioritize fostering environments where staff and faculty are empowered to be a key element of their cybersecurity defenses, equipping them with more than just security awareness training—through proactive cyber defense measures and strong partnerships—create a more resilient and adaptive security culture that can more effectively defend against evolving cyber threats.

The time to act is now. Investing in cybersecurity is about far more than protecting data—it is about safeguarding the futures of students, ensuring educators can teach without disruption, and maintaining the trust and safety of families and communities.

Learn how **the Center for Internet Security makes the connected world a safer place for people, businesses, educational institutions and governments through our core competencies of collaboration and innovation.**

Investing in cybersecurity is not just about protecting data—it is about safeguarding the futures of students, ensuring educators can teach without disruption, and maintaining the trust and safety of families and communities.

CIS Center for Internet Security®

Empowering the Human Element

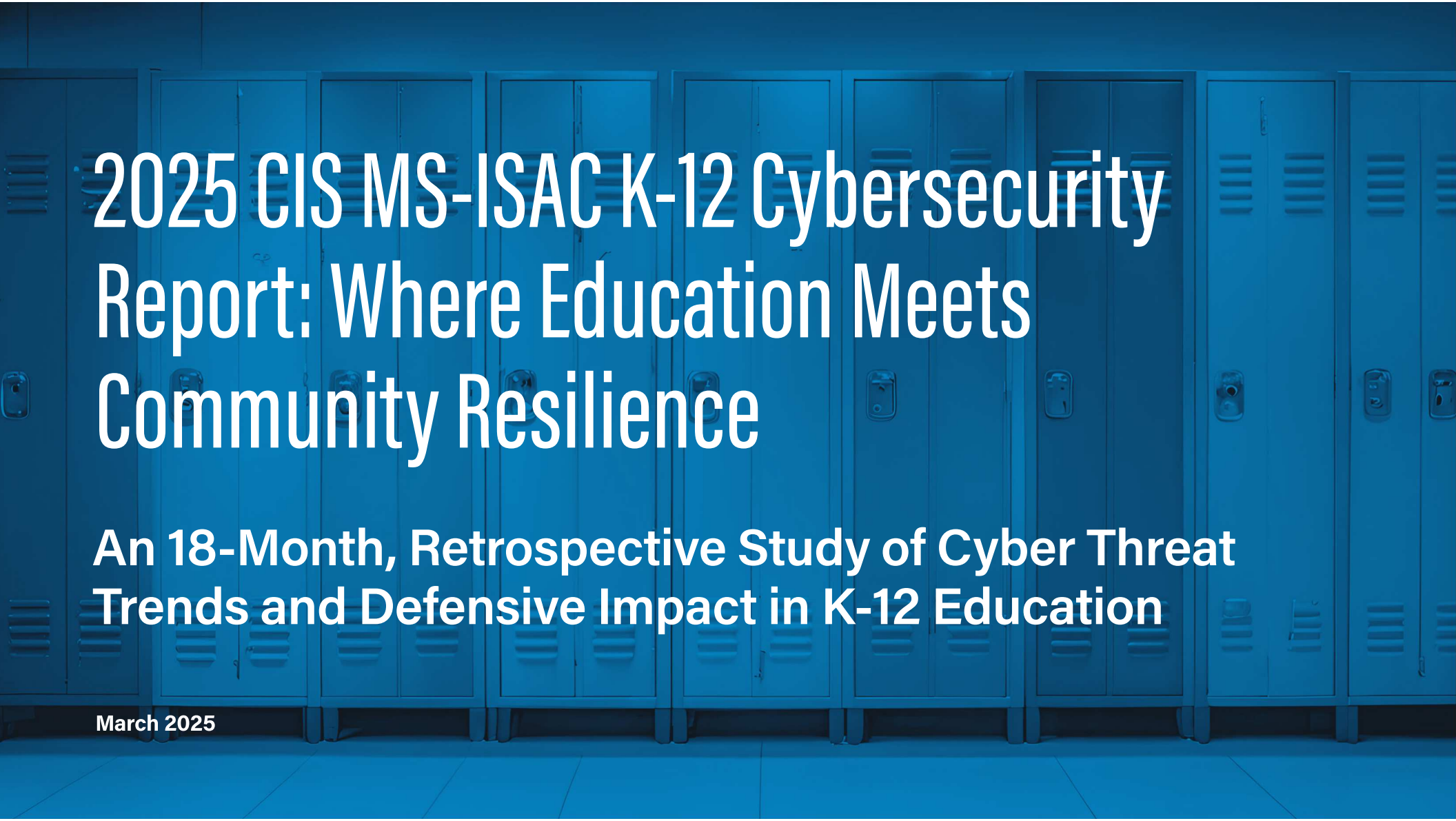
K-12 organizations can achieve stronger cybersecurity by fostering a culture of cyber empowerment. This means ensuring that every individual—from administrators to substitute teachers—understands their role in protecting the school community and feels valued for their contributions. When leadership actively promotes security as a shared responsibility, schools create a more resilient and engaged defense against cyber threats.

CIS Center for Internet Security®

MS-ISAC® Multi-State Information Sharing & Analysis Center®

Contact

www.cisecurity.org
learn@cisecurity.org
518-266-3460



2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience

An 18-Month, Retrospective Study of Cyber Threat Trends and Defensive Impact in K-12 Education

March 2025

Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Produced by Center for Internet Security, in partnership with Consortium for School Networking.

Contents

Where was content sourced for this report?

The following information details the results of an 18-month study covering July 2023 - December 2024. Data for this report was collected from multiple sources, including more than 4,600 K-12 entities in the MS-ISAC. Sources include data collected from respondents to the 2023 and 2024 Nationwide Cybersecurity Review (NCSR), MS-ISAC member feedback, services data, direct reporting data from the CIS Security Operations Center (SOC), data from CIS Cyber Incident Response Team (CIRT) engagements, and threat data and associated analysis by the CIS Cyber Threat Intelligence (CTI) Team.

Who We Are

Every day, the Center for Internet Security, Inc.® (CIS) and Multi-State Information Sharing and Analysis Center® (MS-ISAC®) work alongside K-12 schools in their mission to protect not just computer systems but communities. We understand that when a cyber attack hits a school, it affects far more than just emails and databases — it impacts childrens' access to meals, parents' ability to work, and even community life itself.

CIS® Center for Internet Security®

MS-ISAC® Multi-State Information Sharing & Analysis Center®

Supporting Partner

CoSN Leading Education Innovation

CoSN, the world-class professional association for K-12 EdTech leaders, stands at the forefront of education innovation. We are driven by a mission to equip current and aspiring K-12 education technology leaders, their teams, and school districts with the community, knowledge, and professional development they need to cultivate engaging learning environments. Our vision is rooted in a future where every learner reaches their unique potential, guided by our community.

CoSN represents over 2050 school districts reaching over 11 million students. Our state presence is expanding with 33 CoSN Chapters in 34 states who function at the grassroots level to further effect change and continues to grow as a powerful and influential voice in K-12 education.

Executive Summary

In a small rural district last winter, a ransomware attack struck during midterm exams. As systems went dark, the impact cascaded far beyond the school's digital infrastructure. The cafeteria staff, unable to access their electronic systems, scrambled to feed hundreds of students who depended on school meals. Parents, many working hourly jobs, suddenly needed to find childcare when classes were canceled. The graduating senior class worried about college application deadlines as their transcripts suddenly became inaccessible.

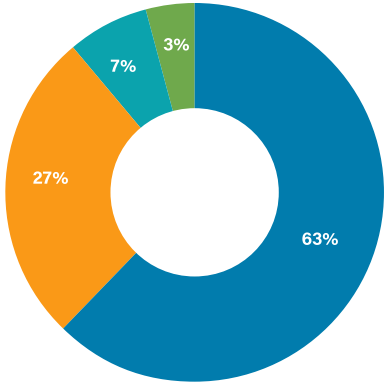
The above scene is an all too common one that has played out in schools across America year after year. Cyber attacks on educational institutions create ripples that affect entire communities. Our analysis of 18 months of data from more than 5,000 K-12 organizations shows that cyber threat actors appear to be increasingly targeting schools during critical periods like exams, times when the pressure to maintain operations makes schools far more vulnerable to ransom demands.

Definition

K-12 organization: Public schools and districts educating students from kindergarten to 12th grade.

Top Malware Infection Vectors

- Malvertisement
- Multiple
- Dropped
- Malspam



The Scale of Impact:

- **82% of K-12 organizations experienced cyber incidents**
- **Nearly 14,000 security events observed**
- **Over 9,300 confirmed incidents**
- **Cyber threat actors target human behavior 45% more often than technical vulnerabilities**

What makes this report's findings particularly troubling goes beyond the number of attacks and confirmed incidents. Rather, we see a significant increase in threat actors' sophistication and timing. We all know that schools serve as essential community infrastructure, and it appears threat actors have also begun to more heavily exploit this fact, as schools provide not just education but vital services:

- Nutritional support through breakfast and lunch programs
- Safe spaces for children of working parents
- Mental health and counseling services
- Special education and developmental support
- Community gathering spaces and resources

When cyber attacks disrupt these services, the effects ripple throughout the community. A parent missing work to care for a child during a school closure creates economic impact. A student missing meals due to cafeteria system outages affects their health and ability to learn. The loss of access to counseling services during critical times can have lasting effects on student well-being.

This report examines how K-12 organizations are responding to these challenges through collaboration, preparation, and a deep understanding that cybersecurity in education is fundamentally about protecting people, not just technology.

Lessons Learned: The Human Cost of Cyber Incidents

When a ransomware attack struck a district during midterm exams in the fall 2024 semester, it revealed a truth about school cybersecurity: these incidents affect far more than just technology. With systems inaccessible, students lost access to meals, parents were forced to arrange childcare, and graduating seniors likely worried about college application deadlines. This scenario, and countless others like it, illustrates what protecting schools from cyber attacks really means — it means protecting communities.

The Human Element: Primary Target

Analysis of incident data reveals a stark reality: cyber threat actors (CTAs) target human behavior exponentially more than any other attack vector. Our services blocked more than 1 billion connection attempts to malvertisement domains and 320 million connection attempts to phishing domains.

Key Findings:

Human-targeted threats exceeded other techniques by 45%

82% of reporting K-12 schools experienced cyber threat impacts

Over 9,300 confirmed incidents

Strategic Timing of Attacks

CIS Cyber Incident Response Team (CIRT) data combined with our security monitoring suggests that CTAs may increase attacks during specific times of the school year. Threat actors appear to ramp up the intensity of their attacks during the beginning of the school year, the mid-term period, and the very end into the summer. These periods could overlap with critical functions such as new staff and student acclimation, mid-term and end-of-year exam weeks, and summer network maintenance periods. Schools face maximum pressure to restore services during critical times, particularly exam periods. The timing of attacks may demonstrate increasing sophistication of cybercriminals and a move toward strategic targeting K-12 organizations during the academic calendar's pressure points.

Beyond the Digital Impact

Not all cyber incidents are created the same, and incidents that lead to schools needing to temporarily shut down impact more than simply the ability to access files.

When cyber incidents force schools to close or limit operations, vital services disappear. The impact extends far beyond missed classes, threatening the basic support systems many families rely on.

Today's K-12 schools serve as more than a place where students prepare for their futures; K-12 schools are essential community infrastructure, enhancing the community by providing:

- Critical nutrition through meal programs.
- Safe spaces for student development.
- Special education and support services.
- Community gathering spaces.
- Extra-curricular activities.
- An increased sense of community.

Collaborative Response Makes a Difference

Schools that engage with the MS-ISAC's no-cost incident response services gain crucial support during cyber incidents. While many incidents go unreported due to a variety of factors (including cyber insurance stipulations and requirements), CIS CIRT data from incidents over the past 18 months indicates that early engagement and preparation significantly improve outcomes.

The K-12 Threat Landscape: An 18-Month Assessment of Risk and Impact

Our comprehensive analysis spanning July 2023 through December 2024 reveals that cyber attacks against schools appear to show tactical patterns. During examination periods across various academic terms, there is a heightened level of threat actor activity. These periods are crucial as they exert significant pressure on schools to sustain their operations amid potential security threats. This extended assessment period provides valuable insights into how attacks evolve across multiple academic cycles.

Patterns of Strategic Targeting

Cyber attacks against schools appear to show tactical patterns. Cyber threat actor activity appears to increase in intensity in relation to specific time periods of the school year, namely during examination periods, critical times during the school year when maintaining day-to-day operations is paramount. This pattern was observed across multiple academic terms. During these high-stakes periods, schools face a seemingly impossible choice: pay a ransom to restore services quickly or potentially compromise students' academic futures.

When a ransomware attack struck during midterm examinations, it revealed how deeply intertwined school technology has become with student success. Teachers lost access to testing materials and student records. Special education services, which rely heavily on detailed digital records and individualized education plans, faced significant disruption.

Impact derived from over 1 trillion logs over 18 months

82% of reporting K-12 schools experienced cyber threat impacts

14,000 Nearly 14,000 security events observed

9,300 Over 9,300 confirmed incidents

The Evolution of Attack Methods

Our analysis shows that attacks targeting human behavior — particularly those through malvertising — exceeded other attack vectors by at least 45%. The trend toward attacks that target human vulnerabilities highlights the adaptability of threat actors, who are now exploiting the inherently supportive and trusting characteristics of educational settings. Teachers, administrators, and support staff, whose primary focus is helping students succeed, now find themselves on the front lines of cybersecurity defense.

How Cyber Threat Actors Exploit Humans in K-12 Settings

- Human-targeted threats exceed technical exploits by 45%
- Malvertisement leads all attack methods
- 66% of schools with endpoint protection affected

Community-Wide Disruption

Modern K-12 schools have evolved into essential community infrastructure, providing vital services that extend far beyond traditional education. When cyber attacks force schools to limit or temporarily cease operations, they don't just interrupt learning — the attack destabilizes the routine of community life itself.

Consider school meal programs, which serve as a critical source of daily nutrition for millions of students. When payment and verification systems go down, schools must choose between turning away hungry students or finding alternative ways to provide meals, all while having the same requirements of tracking the number of students who came through the line. Similarly, when special education programs and counseling services lose access to digital records and communication systems, our most vulnerable students face immediate challenges.

The economic impact ripples throughout the community as parents miss work to care for children who cannot attend school. This disruption particularly affects communities where the school system forms the backbone and routine structure of daily economic activity. A cyber attack on a school doesn't just impact education — it has an outsized effect on the stability and well-being of entire communities.

Collaborative Response: Building K-12 Cyber Resilience Through Partnership

The complexity and impact of cyber threats to K-12 organizations demands a response that extends beyond any single school or district. Our analysis reveals that the most resilient schools embrace a collaborative approach, leveraging partnerships and shared resources to protect their communities.

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

The Power of Proactive Partnership

MS-ISAC membership provides K-12 organizations with crucial support before, during, and after cyber incidents. This no-cost partnership provides schools with access to incident response services, cybersecurity advisory services, threat intelligence, and a network of cybersecurity experts who understand the unique challenges of educational environments.

Consider how these partnerships manifest in practice:

> When schools actively engage with the MS-ISAC and take full advantage of the no-cost and cost-effective resources exclusively available to them as members, they effectively add millions of dollars to their overstretched cybersecurity budgets, getting industry-leading cybersecurity solutions at a fraction of the commercial cost, and in many cases, completely free.

And for K-12 organizations that take the **Nationwide Cybersecurity Review (NCSR) assessment**, their cyber maturity increases by an average of 26%, enabling them to prioritize their limited resources while building defenses that account for both technical and human elements of security.

> Custom threat intelligence derived from within the K-12 sector of membership and broader MS-ISAC community leads to the highest and most impactful detections.
>
> 72% of all Endpoint Detection and Response (EDR) detections and 87% of all EDR incidents were caught from intelligence gathered from our internal investigations and analysis and deployed into the CIS Endpoint Security Services (ESS) environment.

Membership Benefits:

- Access to no-cost incident response services
- Real-time threat intelligence sharing
- Professional development opportunities
- Community-driven best practices
- ...and more.

Integrating Leadership and Technology

For the second year in a row, the Center for Internet Security is proud to see the MS-ISAC and Consortium for School Networking (CoSN) come together and partner on this report, dovetailing our separate missions to strengthen and empower K-12 educational leaders to create a comprehensive approach to school cybersecurity. This collaboration addresses key areas including:

Professional Development	Build capacity among teachers and staff to enable them to recognize and respond to cyber threats while maintaining focus on their primary educational mission.
Resource Optimization	Schools can and should take advantage of no-cost and cost-effective resources and collaborative solutions to help their cybersecurity budgets go further.
Encourage Opportunity in Security	Foster opportunities for smaller and under-resourced districts to access robust cybersecurity solutions, increasing their cyber maturity and helping them better defend against cyber attacks.
Risk Management	Take full advantage of expert-maintained cybersecurity best practices like the CIS Critical Security Controls®. The CIS Controls® balance security needs with educational accessibility, allowing K-12 organizations to apply controls in a manner that best addresses the challenges of their organization's unique environment.

Opportunities for Creating Resilient Communities

The most effective defense strategies recognize that school cybersecurity extends beyond protecting digital assets; it's about preserving the educational and social infrastructure that communities depend on.

This understanding drives the development of:

Response Networks

Schools can build connections with community organizations that can help maintain essential services during cyber incidents.

Communication Channels

K-12 organizations should establish clear protocols for keeping families and community members informed during security events.

Service Continuity

Schools should develop and regularly audit service continuity plans to maintain critical community services, especially for vulnerable populations, even when digital systems are compromised.

Recommendations: Protecting Schools, Preserving Communities

In developing cybersecurity recommendations for K-12 organizations, we understand that we must fundamentally shift how we think about the human element in cybersecurity. Our analysis shows that the most successful approaches treat people not as vulnerabilities to be managed, but rather, as powerful assets to be empowered.

Empowering the Human Element

Our research shows that K-12 organizations can achieve significantly better security outcomes when they instead foster an environment where every individual understands their vital role in protecting their school community.

While cybersecurity measures often focus on the technical aspects of securing the environment, integrating a human-first approach to security mirrors what K-12 organizations are already doing to address types of threats such as tornadoes or fires.

Creating a Culture of Cyber Empowerment

K-12 organizations should develop environments where everyone who accesses the network — from administrators to substitute teachers — feels they are a crucial part of the security team. What this means in practice is K-12 organizations should strive to:

- Build a shared understanding that every individual plays an active role in protecting students, families, and community services.
- Recognize and celebrate when staff members identify and report potential security concerns.
- Create open dialogue between IT security teams and educational staff to better understand each other's needs and challenges.
- Ensure all members of the school community understand how their actions directly contribute to protecting vital services.

Increasing Cyber Maturity Through Frameworks

The CIS Critical Security Controls (CIS Controls) are a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture. Today, thousands of cybersecurity practitioners from around the world use the CIS Controls and/or contribute to their development via a community consensus process.

> The traditional view of humans as the "weakest link" in cybersecurity has created a self-fulfilling prophecy in many organizations. When we consistently tell people they are a liability, they often unconsciously fulfill that role.

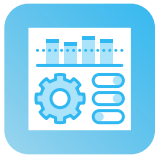
Moving Beyond Traditional Awareness

While security awareness training has its place, it should be viewed as just one small part of a larger cultural transformation. K-12 organizations should focus their efforts to:

- Develop collaborative relationships between IT security teams and educational staff, where both groups work together to find solutions that protect both security and educational needs.
- Create clear, accessible channels for staff to report concerns without fear of judgment or reprisal.
- Provide regular feedback to staff about how their vigilance and actions have helped protect the school community.
- Ensure leadership actively demonstrates that security is a shared responsibility, not just an IT concern.

Technical Framework Development

When technical controls complement and support human empowerment, rather than restrict and frustrate, organizations build stronger security. K-12 organizations should implement technology solutions that protect both their community and their mission.



Essential Security Controls

Security technology should enable and protect educational activities while remaining as frictionless as possible to users. Key implementations include:

- Multi-factor authentication designed with teacher workflows in mind, understanding that educators often need quick access while moving between classrooms or helping students.
- Backup systems that automatically protect critical data while allowing teachers to focus on teaching rather than manual backup procedures.
- Network design that protects sensitive information while ensuring teachers and staff can efficiently access the resources they need.
- Endpoint protection that focuses on preventing threats without creating barriers to educational software and resources.

Service Continuity Planning

Technical planning should prioritize maintaining essential community services during cyber incidents. Every organization is different, so the following recommendations are representative rather than prescriptive:

- Work with cafeteria staff to develop systems that keep meal programs running even if networks are compromised.
- Collaborate with teachers to create accessible backup copies of critical student records.
- Design emergency communication systems that staff can easily use during incidents.
- Maintain simple, paper-based backup procedures that staff can confidently implement when needed.

Strengthening Through Partnership

Partnerships multiply the effectiveness of both human and technical security measures. When organizations work together, they create networks of support that enhance everyone's resilience.

MS-ISAC Collaboration

MS-ISAC membership provides more than just technical tools — members establish connections that empower them. With a notification time 92% faster, on average, than most other MSSPs, the MS-ISAC delivers unparalleled value to members. Additionally, MS-ISAC members can:

- Access immediate support during incidents from cybersecurity and incident response experts who understand K-12 environments.
- Share insights and experiences with peer organizations facing similar challenges.
- Implement security monitoring that supplements local expertise.
- Build relationships with the broader K-12 cybersecurity community and other local government entities before crises occur.

Professional Growth

Professional development should focus on building confidence in addition to capability:

- Engage with CoSN to develop both technical skills and educational leadership.
- Practice incident response through collaborative tabletop exercises that build team confidence.
- Create opportunities for staff to feel heard and invite them to share their security experiences and insights.
- Identify and support staff members who show interest in becoming security advocates.

Fostering Community Resilience

Strong communities can help schools weather cyber incidents, but it is not automatic. K-12 schools must intentionally strengthen these relationships. Building these relationships requires:

Communication Development

Create communication strategies that:

- Establish trusted channels for sharing information with families during incidents.
- Build relationships with local media to ensure accurate, helpful coverage of your organization — whether your team just won the state tournament or your operations have been impacted by a cyber incident.
- Prepare clear, accessible templates for various types of incidents and implement these templates into your tabletop exercises to get real-world experience and gain confidence.
- Maintain strong connections with community partners who can provide support to your K-12 organization in the event of a cyber incident.

Service Protection

When a cyber attack impacts your ability to provide services — education, meals, activities, transportation — the fallout can be enormous. Prioritize protecting these essential services through active community engagement:

- Work with staff to identify the most critical services your school provides.
- Develop practical alternatives for maintaining these services with minimal disruption during incidents.
- Build partnerships with community organizations who can provide backup support.
- Create clear guidelines for service continuity that empower staff to make decisions.

Conclusion: Building Resilient Educational Communities Together

The challenges facing K-12 organizations and their cybersecurity extend far beyond protecting data and devices. When cyber incidents strike schools, they threaten the essential services that bind communities together. Our 18-month analysis reveals that schools serve as crucial community infrastructure, providing nutrition, safety, support services, and educational opportunities that families depend on every day.

Traditional approaches to cybersecurity have often treated humans as a weakness to be mitigated through training and restrictions. Thankfully, cybersecurity experts are realizing a new, more human-empowering approach is needed. The most resilient organizations take this fundamentally different approach. They recognize that their people — from teachers and administrators to support staff and technical teams — represent their greatest security asset when effectively empowered and supported.

This seismic shift from viewing people as liabilities to seeing them as essential defenders transforms how organizations approach security. When staff members feel valued and understand their crucial role in protecting their school community, they are more likely to become active participants in security rather than passive recipients of compliance-focused training. They develop the confidence to identify threats, the knowledge to respond effectively, and the understanding that their actions directly protect students, families, and essential services that extend far beyond the classroom.

The technical controls and partnerships we've discussed can make a significant difference,, and they function best when implemented in service of this human-centered approach. Multi-factor authentication, backup systems, and monitoring tools should support educational missions rather than impede them.

When K-12 organizations partner with organizations like the MS-ISAC and CoSN, they build capability and confidence alongside technical expertise.

The future is bright, and the path is well-lit, but the journey requires continued, intentional commitment to:

- Understanding schools as essential community infrastructure that provides vital services beyond education.
- Empowering every individual who accesses school networks to become an active defender of their community.
- Implementing technical controls that protect services while supporting educational missions.
- Building partnerships that enhance both human and technical capabilities.
- Creating resilient communities that can maintain essential services even during cyber incidents.

As we look to the future, the cybersecurity challenges facing K-12 organizations will undoubtedly evolve, but so will you. By fostering environments where every individual feels empowered to protect their school community, implementing supportive technical controls, and building strong partnerships, your organization can develop the resilience needed to face these challenges while continuing to serve your community.

Key Takeaways:

- **Schools are essential community infrastructure.**
- **Empowered humans are the strongest line of defense.**
- **Technical controls should support educational missions.**
- **Partnerships multiply organizational capabilities.**
- **Community resilience depends on maintaining essential services.**

Appendices

Appendix A: Understanding MS-ISAC Services for K-12 Organizations

The Multi-State Information Sharing and Analysis Center (MS-ISAC) provides:

CYBERSECURITY SERVICES	DESCRIPTION	NO COST	COST EFFECTIVE
Cyber Threat Intelligence			
Cyber Alerts and Advisories	Brief, timely emails containing information on specific cyber incidents/threats and vulnerabilities in software and hardware	✓	
Quarterly Threat Reports	Analysis of SLTT-focused cyber threat intelligence trends and threat forecasting	✓	
Regular IOCs	Weekly, monthly reports on malicious IPs/domains	✓	
White Papers	Technical papers providing relevant information on cyber threat topics	✓	
Cyber Threat Briefings	Informative sessions on the cyber threat landscape to SLTTs	✓	
Real-time Intelligence Feeds	Easy-to-implement real-time cyber threat intelligence indicator feeds derived from more than 200 sources and specific to SLTTs	✓	
Cybersecurity Services			
24x7x365 Security Operations Center (SOC)	Full-time cyber defense partner to member organizations that monitors, analyzes, and responds to cyber incidents affecting members	✓	
Malicious Domain Blocking & Reporting (MDBR)	Web security service that proactively blocks network traffic to known harmful web domains, protecting IT systems against cyber threats	✓	
Endpoint Security Services (ESS)	Device-level protection and response for active defense against both known (signature-based) and unknown (behavioral-based) malicious activity		✓
Albert Network Monitoring and Management	Cost-effective network Intrusion Detection System (IDS) tailored to SLTT governments' threat profile and security needs		✓
Managed Security Services (MSS)	Cost-effective log and security event monitoring of devices like IDS/IPS, firewalls, switches and routers, services, endpoints, and web proxies		✓
Penetration Testing	Services that simulate real-world cyber attacks on network and web applications and enable organizations to safely identify exploitable vulnerabilities		✓

Appendices

Appendix A: Understanding MS-ISAC Services for K-12 Organizations (continued)

CYBERSECURITY SERVICES	DESCRIPTION	NO COST	COST EFFECTIVE
Security Best Practices			
CIS SecureSuite Membership	Comprehensive set of cybersecurity resources and tools to implement the CIS Critical Security Controls (CIS Controls) and CIS Benchmarks	✓	
Other Member Services and Resources			
MS-ISAC Webinars	Monthly member calls and webinars on topics of interest to the SLTT community	✓	
MS-ISAC Working Groups	Voluntary committees focused on collaboration among SLTT organizations to help drive MS-ISAC initiatives and member enrichment and growth	✓	
Nationwide Cybersecurity Review (NCSR)	Anonymous, annual self-assessment designed to evaluate cybersecurity maturity and set a baseline for organizational improvement	✓	
CIS CyberMarket	A collaborative purchasing program available to SLTTs that leverages collective purchasing power of our 16,000+ member organizations to provide low-cost security solutions from industry-leading cybersecurity providers		✓

Appendix B: Building Your Security Program

This section provides a scalable framework for establishing and maintaining an effective K-12 security program that empowers your educational community.

Program Elements	
Leadership Engagement	• Establish security as a school-wide priority • Champion active support for security initiatives • Allocate resources effectively
Community Integration	• Identify essential services your school provides • Map dependencies between services • Create service continuity plans
Technical Implementation	• Deploy fundamental security controls • Establish monitoring capabilities • Maintain backup systems
Partnership Development	• Engage with security organizations • Build local support networks • Share experiences with peer institutions

Appendix C: Resource Guide

Take advantage of the resources available to your organization. These resources have been developed by cybersecurity and threat intelligence experts and are maintained by dedicated teams of security professionals around the country and around the world.

Resource	
Incident Response Plan Template	Access Incident Response Plan Template
CIS Critical Security Controls®	https://www.cisecurity.org/controls
CIS Benchmarks®	https://www.cisecurity.org/cis-benchmarks
CIS Hardened Images®	https://www.cisecurity.org/cis-hardened-images

Appendix D: Glossary of Terms

This glossary provides clear, non-technical explanations of key concepts referenced throughout the report.

Glossary

Incident Response	The organized approach to addressing and managing the aftermath of a security breach or cyber attack.
Malspam	Email-based attacks wherein emails contain attachments or links that contain or deliver malicious software (malware).
Malvertisement	An attack tactic that uses internet advertisement space maliciously to spread malware and compromise systems.
Multi-factor Authentication (MFA)	A security method requiring users to provide two or more verification factors to gain access to a resource.
Ransomware	Malicious software that encrypts files, making them inaccessible until a ransom is paid.
Service Continuity	The capability of an organization to continue delivery of essential services at acceptable levels following a disruptive incident.

Appendix E: Nationwide Cybersecurity Review Results

2024 Nationwide Cybersecurity Review (NCSR)

The 2024 Nationwide Cybersecurity Review (NCSR) assessment is available to complete from October 2024 through February 2025. The below data reflects NCSR assessment submissions between October 2024 and December 2024.

286 K-12 school districts completed the NCSR assessment during this timeframe.

Here are aggregate data findings for the K-12 participants during this timeframe, as well as comparisons to historical data.

Top 5 Security Concerns

Lack of Sufficient Funding	a. 86% of K-12 participants selected in the 2024 NCSR b. 82% of K-12 participants selected in the 2023 NCSR
Increasing Sophistication of Threats	a. 61% of K-12 participants selected in the 2024 NCSR b. 61% of K-12 participants selected in the 2023 NCSR
Lack of Documented Processes	a. 52% of K-12 participants selected in the 2024 NCSR b. 53% of K-12 participants selected in the 2023 NCSR
Lack of a Cybersecurity Strategy	a. 37% of K-12 participants selected in the 2024 NCSR b. 38% of K-12 participants selected in the 2023 NCSR
Inadequate Availability of Cybersecurity Professionals	a. 32% of K-12 participants selected in the 2024 NCSR b. 37% of K-12 participants selected in the 2023 NCSR

K-12 School District Staffing

2024 86% of K-12 school districts stated they have less than 5 employees with security related duties.

2023 89% of K-12 respondents in the 2023 NCSR cycle stated they have less than 5 employees with security related duties.

K-12 Overall Maturity Scoring

2024 The overall average maturity score of K-12 NCSR participants was 3.76 on the NCSR's 1 through 7 scoring scale.

2023 This was an improvement compared to the 2023 NCSR cycle's average maturity score of 3.45

- The 2023 cycle average fell below the score of other local level sectors, such as public utilities, health services, and election offices.

K-12 School Districts & Security Framework Usage

2024 77% of K-12 school districts stated they use a security framework, such as the CIS Controls or the NIST Cybersecurity Framework (CSF).

- K-12 school districts that use a security framework scored 26% higher, on average, compared to those not using a framework.

2023 73% of K-12 respondents stating they use a framework during the 2023 NCSR cycle. K-12 schools using a framework scored 52% higher at that time.

K-12 High-Performing Areas

NIST Cybersecurity Framework (CSF) Categories:

- Protect: Identity Management & Access Control
- Respond: Mitigation
- Protect: Awareness and Training
- Detect: Security Continuous Monitoring
- Respond: Analysis

2023 The top three categories were the same compared to the 2023 NCSR cycle. The two changes within the top five scoring categories were the "Detect: Security Continuous Monitoring" category entering the top five, as well as the "Respond: Analysis" category entering the top five.

Specific Activity Areas:

- Having an inventory of physical devices and systems
- Managing and verifying identities/credentials for authorized users
- Managing remote access

K-12 Lower-Performing Areas

NIST Cybersecurity Framework (CSF) Categories:

- Identify: Risk Management Strategy
- Protect: Protective Technologies
- Detect: Anomalies & Events
- Recover: Improvements
- Recover: Communications

2023 The two changes within bottom five scoring categories were the "Recover: Improvements" category and the "Recover: Communications" category entering the bottom five.

Specific Activity Areas:

- Protecting and restricting use of removable media
- Detecting unauthorized mobile code
- Establishing and managing organizational risk tolerance
- Usage of integrity checking mechanisms to verify software integrity
- Aggregating and correlating event data from multiple sources and sensors
- Separating the development and testing environment(s) from the production environment

K-12 Lower-Performing NCSR Areas Aligned to CIS Controls

Note: The below details are more granular than the information earlier in this document, as it views specific NIST Cybersecurity Framework (NSF) subcategory activities aligned to the CIS Controls and applicable Control Safeguards.

NIST CSF Category	CIS Critical Security Control	Recommended Actions
Protect: Protective Technologies	**CIS Control 3:** Data Protection	• Establish and Maintain a Data Classification Scheme • Document Data Flows • Encrypt Data on Removable Media
	CIS Control 8: Audit Log Management	• Collect Audit Logs • Standardize Time Synchronization • Collect Command-Line Audit Logs • Conduct Audit Log Reviews
	CIS Control 10: Malware Defenses	• Disable Autorun and Autoplay for Removable Media
Recover: Communications	**CIS Control 17:** Incident Response Management	• Establish and Maintain Contact Information for Reporting Security Incidents • Define Mechanisms for Communicating During Incident Response

For a look at the previous year's NCSR data, see 2023 Nationwide Cybersecurity Review: https://learn.cisecurity.org/NCSR-2023-Summary-Report .

Appendix F: CTI Team Writeup with Data

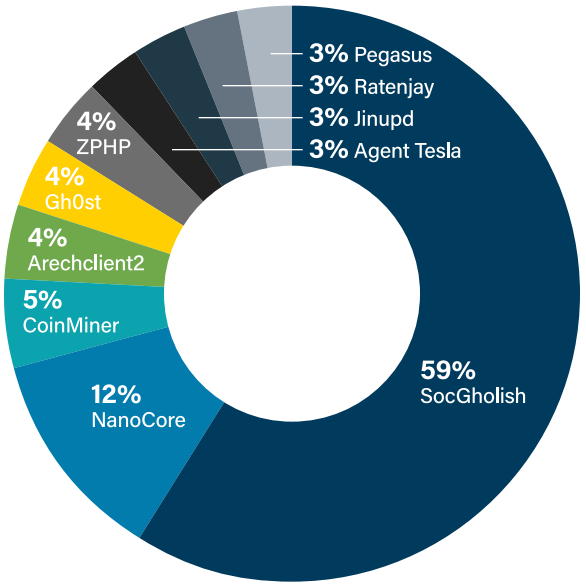
Top 10 Malware Affecting K-12 Schools

CIS, through the MS-ISAC, maintains the largest database for security threats against U.S. SLTT governments, including K-12 schools. This SLTT specific threat database is informed by Albert IDS telemetry.

From July 2023 through December 2024, SocGholish was the top malware affecting K-12 entities, making up 60% of the top 10 malware. This contrasts with the previous year where QakBot, a modular banking trojan, posed the most significant threat to K-12 entities. The year to year change is due to the end of QakBot's campaign and the beginning of a large scale SocGholish malware campaign. The second and third most prevalent malware were NanoCore and CoinMiner. The top 10 malware had a 50% change compared to the previous K-12 report, with the new additions being: SocGholish, NanoCore, ZPHP, Jinupd, and Pegasus.

> From July 2023 through December 2024, SocGholish was the top malware affecting K-12 entities, making up 60% of the top 10 malware.

SocGholish is a downloader written in JavaScript which is distributed through malicious or compromised websites. SocGholish uses fake software updates, specifically browser updates, to trick users into downloading the malware. The malware uses multiple methods for traffic redirection and payload delivery. After initial infection, the cyber threat actors (CTAs) use Cobalt Strike, leverage PowerShell, and steal information from the victim's system. Additionally, SocGholish infections can lead to further exploitation, such as installing the NetSupport remote access tool, AsyncRAT, and ransomware in some cases.

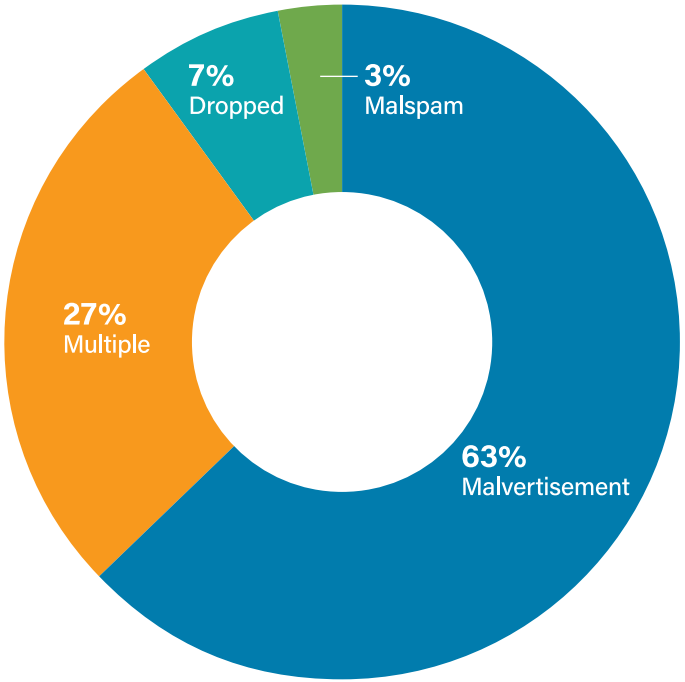


NanoCore is a Remote Access Trojan (RAT) sold on the dark web and is typically spread via malspam with an attachment. NanoCore has keylogging and screen capture capabilities, steals passwords, can download and execute files, exfiltrate data, and adds registry keys for persistence.

CoinMiner is a cryptocurrency miner family that typically uses Windows Management Instrumentation (WMI) to spread across a network. Additionally, it often uses the WMI Standard Event Consumer scripting to execute scripts for persistence. However, the malware's capabilities vary as there are multiple variants. CoinMiner spreads through malspam or is dropped by other malware.

How Cyber Attackers Gain Access

CIS tracks potential initial infection vectors for the Top 10 Malware each quarter based on open-source reporting, as depicted in the graph below. We currently track four initial infection vectors: Dropped, Malvertisement, Malspam, and Network. Some malware uses different vectors in different contexts and are tracked as Multiple.



Malvertisement made up 63% of the top malware initial infection vectors prodominately due to the ongoing SocGholish campaign. Multiple, which was the top initial infection vector in last year's report, continues to increase and make up a significant percentage due to CTAs utilizing more than one vector to increase their chances of success. The most popular combination for the multiple initial infection vector is malspam and dropped. Dropped and malspam continue to close out the rest of the top 10 malware initial infection vectors.

63%

Malvertisement

Malware introduced through malicious advertisements. Malware currently using this technique include SocGholish and ZPHP.

27%

Multiple

Malware that currently uses at least two vectors, such as dropped and malspam. Malware currently using this technique include Amadey, ArechClient2, CoinMiner, and Lumma Stealer.

7%

Dropped

Malware delivered by other malware already on the system, an exploit kit, infected third-party software, or manually by a CTA. Malware currently using this technique include Gh0st and Ratenjay.

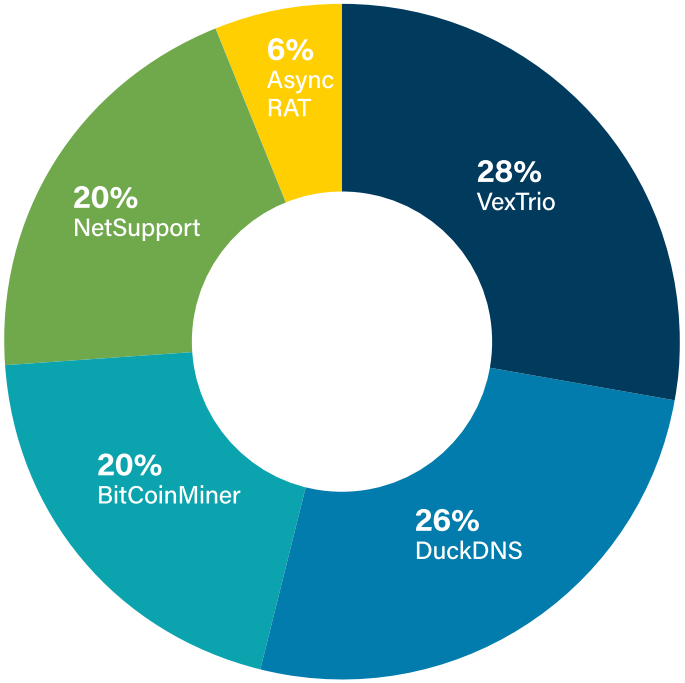
3%

Malspam

Unsolicited emails, which either direct users to malicious websites or trick users into downloading or opening malware. Malware currently using this technique include Agent Tesla and Tinba.

Top 5 Non-Malware

CTAs are increasingly leveraging legitimate remote monitoring and management tools to access and control victims' machines. By expanding their use of legitimate tools, CTAs are more effective at making their presence on a network appear legitimate, effectively hiding their activity among all the other legitimate activities and processes. Four of the top 5 non-malware threats are legitimate tools or services, making up 72% of the top 5 non-malware threats. These legitimate tools or services include: AsyncRAT, BitCoinMiner, DuckDNS, and NetSupport.



From July 2023 through December 2024, three of the top 5 non-malware changed from the previous year's MS-ISAC K-12 Cybersecurity Report, with the exception of AsyncRAT and NetSupport. The top two non-malware threats affecting K-12 entities were VexTrio and BitCoinMiner, making up 54% of the top 5 non-malware. VexTrio led the top 5 non-malware due to being used by multiple malware campaigns, such as SocGholish. BitCoinMiner moved to the second spot which is likely due to the surge in the price of bitcoin over the past year.

VexTrio is the name of a CTA traffic broker group as well as the group's infrastructure. They operate traffic distribution systems (TDSs), as well as their own infrastrucutre. VexTrio also sells the use of their TDSs to affiliate CTAs, which is known as TDS-as-a-Service. Affiliate CTAs will direct traffic from compromised websites to the VexTrio TDS infrastructure, which is then redirected to various malicious websites based on the traffic profile attributes.

DuckDNS is a legitimate DDNS or dynamic DNS serivce. DuckDNS is a free service which will point a DNS (subdomain of duckdns[.]org) to an IP address of your choice. However, CTAs often use DuckDNS service, as well as other services like DuckDNS, to deliver malware and for comand and control infrastructure.

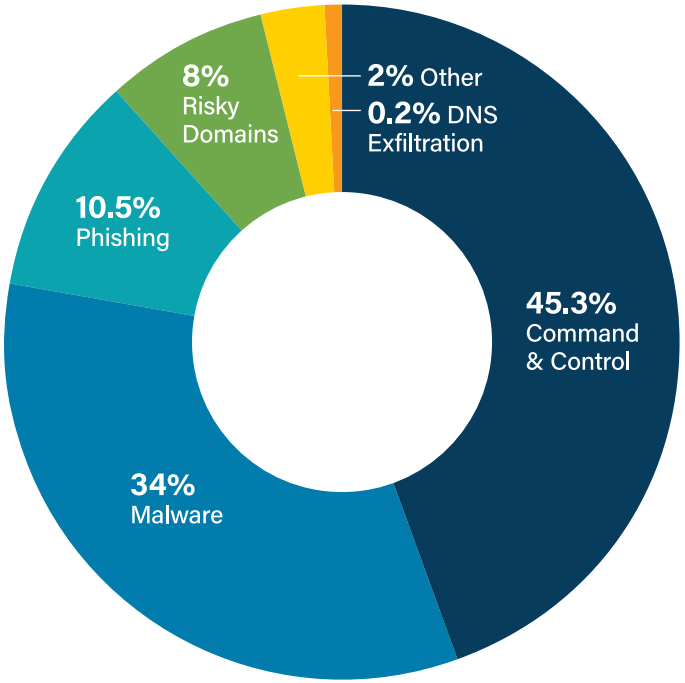
BitCoinMiner is a legitimate cryptocurrency miner that CTAs are deploying on unauthorized computers and networks. BitCoin Miners utilize the processing power of the host machine to mine BitCoin, which degrades the performance on the host for legitimate applications.

Four of the top 5 non-malware threats are legitimate tools or services, making up 72% of the top 5 non-malware threats. These legitimate tools or services include: AsyncRAT, BitCoinMiner, DuckDNS, and NetSupport.

K-12 Web Security Trends

The Malicious Domain Blocking and Reporting (MDBR) service is a secure recursive DNS solution offered at no cost to K-12 schools. MDBR prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats.

Between July 2023 through December 2024, command and control ("C&C") overtook "malware" as the top-ranking spot for MDBR blocked activity. C&C activity increased year over year by 1,552%, while Malware blocked activity increased by 443%. Although Malware activity did increase over the past year, it did not increase enough to keep the top spot.



Between July 2023 through December 2024, command and control ("C&C") overtook "malware" as the top ranking spot for MDBR blocked activity.

Appendix G: Contributors

Center for Internet Security thanks the following contributors, without whom this report would not have come to fruition:

CIS Cyber Threat Intelligence Team: The Cyber Threat Intelligence Team provided essential insights and analysis, enhancing the report's depth and accuracy.

CIS Cyber Incident Response Team: The Cyber Incident Response Team's expertise in incident handling and response contributed to the report's understanding of emerging threats and vulnerabilities.

CIS Security Operations Center Team: The Security Operations Center Team's continuous vigilance and monitoring efforts supported the report's emphasis on proactive threat mitigation.

CIS Nationwide Cybersecurity Review Team: The Nationwide Cybersecurity Review Team's data collection and analysis efforts formed the foundation of this report, enabling us to present comprehensive findings.

CIS Stakeholder Engagement Operations Team: The Stakeholder Engagement Operations Team ensured that the report's insights would be disseminated effectively to stakeholders and partners.

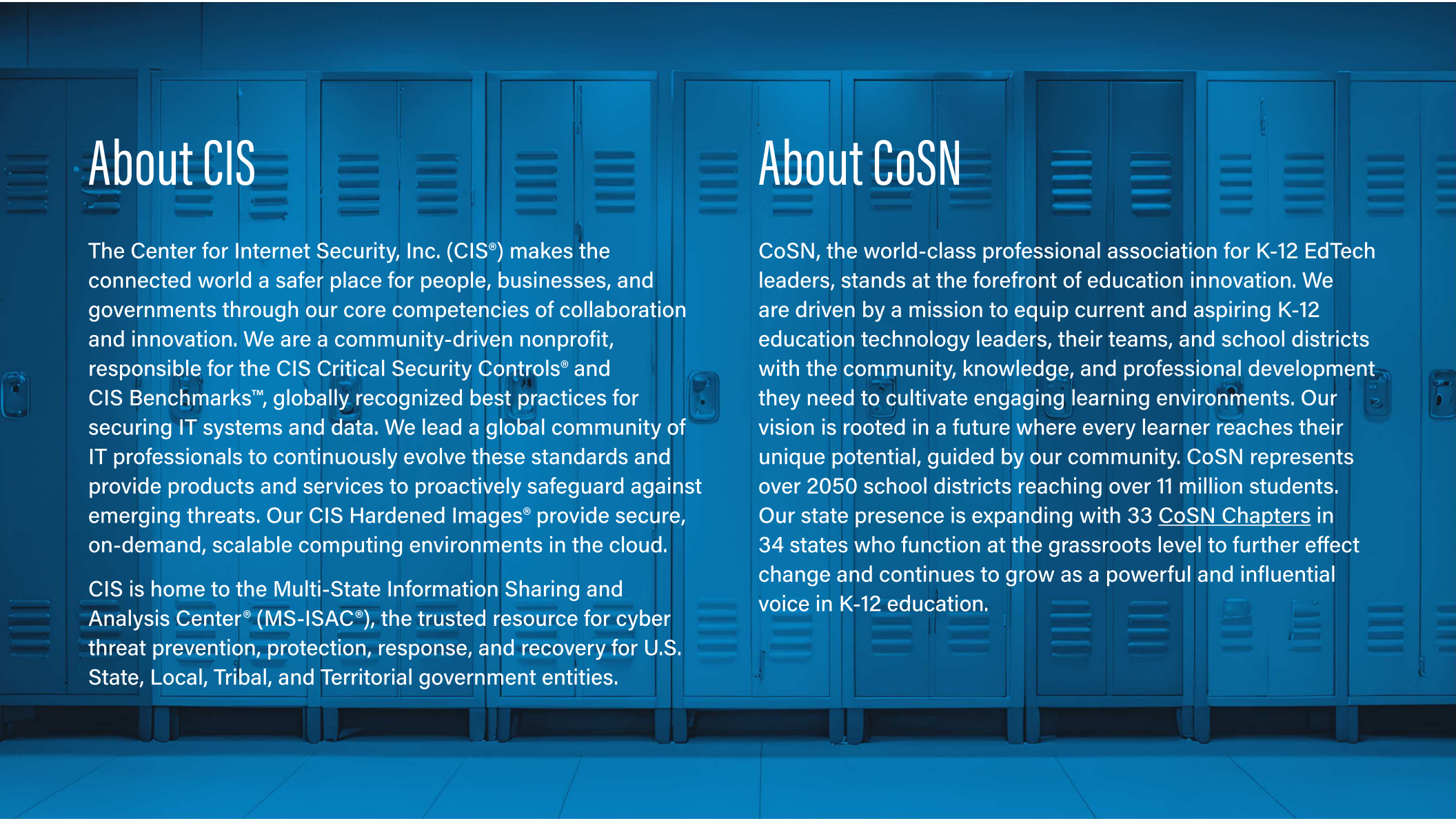
CIS Marketing and Communications Team: The Marketing and Communications Team played a pivotal role in crafting and conveying the message of this report, ensuring its clarity and reach.

We extend our sincere thanks to everyone involved in this project for their dedication, expertise, and unwavering support. The value your commitment brings to helping K-12 organizations increase their cyber maturity cannot be overstated. Thank you!

Special Thanks

We'd like to thank our K-12 MS-ISAC members for their strong collaboration and hard work to improve cybersecurity across this vital community.

We'd also like to extend our gratitude to Consortium for School Networking (CoSN) for their commitment to empowering K-12 leaders to succeed in the digital transformation through resources and advocacy tools. Special thanks to the CoSN and the CoSN Cybersecurity Advisory Committee for their outstanding support for, and contribution to, this report.



About CIS

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities.

About CoSN

CoSN, the world-class professional association for K-12 EdTech leaders, stands at the forefront of education innovation. We are driven by a mission to equip current and aspiring K-12 education technology leaders, their teams, and school districts with the community, knowledge, and professional development they need to cultivate engaging learning environments. Our vision is rooted in a future where every learner reaches their unique potential, guided by our community. CoSN represents over 2050 school districts reaching over 11 million students. Our state presence is expanding with 33 CoSN Chapters in 34 states who function at the grassroots level to further effect change and continues to grow as a powerful and influential voice in K-12 education.

CIS Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security

@CISecurity
TheCISecurity
cisecurity