K-12 Report

CIS MS-ISAC Cybersecurity Assessment of the 2022–2023 School Year

November 2023

CIS® Center for Internet Security®

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

Contents

Who is this report for?

This report offers K-12 leaders, including superintendents, principals, and administrative staff, as well as IT leaders and cybersecurity practitioners, valuable industry-specific insights to inform their decisions regarding cyber risk. The information in this report can also help IT and cybersecurity professionals responsible for their organization's cybersecurity maturity better prioritize cyber defense measures to keep up with evolving cyber threats targeting K-12 organizations.

Where was content sourced for this report?

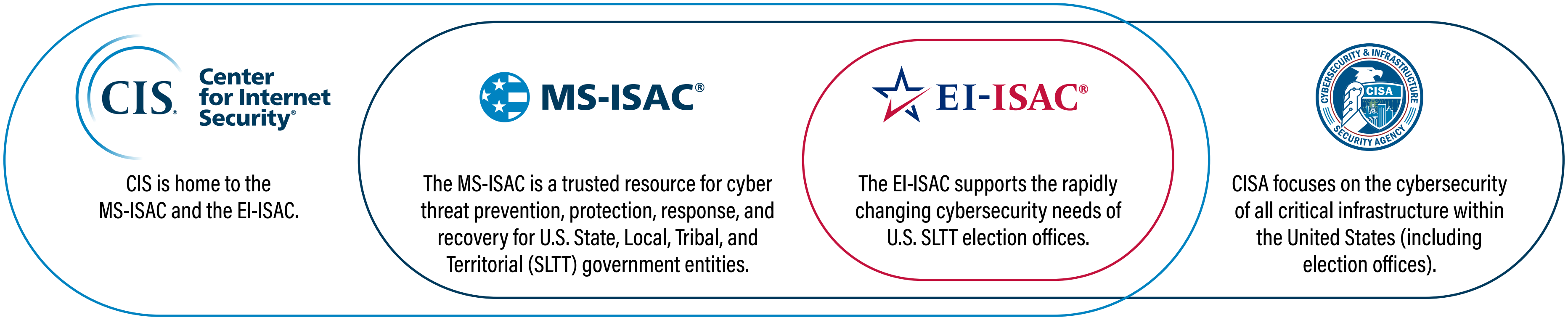
The following information details first-hand reported data from the 2022-2023 school year, as submitted to the MS-ISAC from multiple sources, including more than 4,600 K-12 entities in the MS-ISAC. Sources include data collected from 402 respondents to the 2022 Nationwide Cybersecurity Review (NCSR), MS-ISAC member feedback, service, direct reporting data from the CIS Security Operations Center (SOC), and threat data and associated analysis by the CIS Cyber Threat Intelligence (CTI) Team.

Who We Are

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. CIS is a community-driven nonprofit, responsible for the 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. 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.

The MS-ISAC is federally funded by CISA and a division of the Center for Internet Security (CIS). The MS-ISAC is autonomously guided by its Executive Committee and member organizations. The mission of the MS-ISAC is to improve the overall cybersecurity posture of over 16,000 U.S. State, Local, Tribal, and Territorial (SLTT) government organizations through coordination, collaboration, cooperation, and increased communication. The MS-ISAC offers members no-cost incident response and remediation support through our team of security experts and develop tactical, strategic, and operational intelligence, along with advisories that offer actionable information for improving organizational cyber maturity.

The Nationwide Cybersecurity Review (NCSR) is a no-cost, anonymous, annual self-assessment. All states (and agencies), local governments (and departments), tribal nations, and territorial governments are encouraged to participate. It is designed to measure gaps and capabilities of SLTT governments' cybersecurity programs and is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).



CIS is home to the MS-ISAC and the EI-ISAC.

The MS-ISAC is a trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

The EI-ISAC supports the rapidly changing cybersecurity needs of U.S. SLTT election offices.

CISA focuses on the cybersecurity of all critical infrastructure within the United States (including election offices).

Executive Summary

K-12 leaders and IT and cyber professionals have faced significant challenges over the last several years. The complexities of shifting between in-person, virtual, and hybrid schooling have been met with an increasingly complicated and evolving cyber threat landscape where K-12 schools have become primary targets of cyber threat actors (CTAs). At the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), K-12 schools represent more than a quarter of our 16,000+ member organizations across the country.

If your school or district is not currently a member of the MS-ISAC, you're missing out on some powerful no-cost and low-cost tools and resources to assist your cybersecurity program. Learn more at www.cisecurity.org/ms-isac/.

The Center for Internet Security, Inc. (CIS®) collected first-hand data for the 2022-2023 school year through the Nationwide Cybersecurity Review (NCSR), feedback from MS-ISAC members, and data from the CIS Security Operations Center (CIS SOC). This data empowers K-12 leaders to make informed decisions regarding cyber risk and provides K-12 IT and cybersecurity professionals with a comprehensive understanding of the cyber threat landscape and practical guidance for improving cyber defenses. Key report highlights include:

Nationwide Cybersecurity Review (NCSR) Assessment: According to the assessment responses, the K-12 districts' leading concern is insufficient funding and inadequate cybersecurity resources.

Maturity Findings: K-12 schools are performing well in Identity Management and Access Control, Awareness and Training, and Maintenance; however, they report the lowest maturity in Protective Technologies, Information Protection Processes & Procedures, Supply Chain Risk Management, and Detection Processes.

Ransomware Findings: Ransomware continues to be one of the top concerns for K-12 organizations, so organizations should prepare and test for the efficacy of their incident response plans to limit the scope and impact before a full-blown attack.

Top 10 Malware: Qakbot, CoinMiner, and Tinba were the top three malware families affecting K-12 schools.

Top 5 K-12 Non-Malware Threats: The top two non-malware threats affecting K-12 entities were AsyncRAT and MageCart.

K-12 Web Security Trends: Malware still ranks as the most blocked threat in MDBR.

COSN EdTech Survey: Survey results revealed that cybersecurity was the number-one priority this year and budget constraints remain the number-one challenge facing EdTech Leaders.

K-12 Community Assessment

Now in its 20th year, the MS-ISAC supports more than 16,000 organizational members from among U.S. State, Local, Tribal, and Territorial (SLTT) governments. More than 4,600 of these members are K-12 schools and districts. K-12 has been the fastest-growing MS-ISAC member segment for the past four years. While the cyber threat against K-12 schools has increased significantly since 2020, these important organizations continue to face the challenges of limited technical staff and financial resources to enact cybersecurity measures.

Top Five Security Concerns

K-12 respondents to the 2022 NCSR reported their top five security concerns as follows:

Lack of sufficient funding	81% **of participants**
Increasing sophistication of threats	59% **of participants**
Lack of documented processes	58% **of participants**
Lack of a cybersecurity strategy	47% **of participants**
Inadequate availability of cybersecurity professionals	41% **of participants**

Data timeframe: July 1, 2022 – June 30, 2023

From the 2021 NCSR to the 2022 assessment, K-12 institutions consistently identified the same top five security concerns, with the leading concern being insufficient funding.

Staffing, Frameworks, Recovery Planning, and Reporting

K-12 School District Staffing

90% of K-12 school districts stated they have less than 5 employees with security-related duties.

K-12 School Districts and Security Framework Usage

68% of K-12 school districts stated they use a security framework, such as the CIS Critical Security Controls (CIS Controls) or the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). On average, K-12 school districts that use a security framework scored 36% higher on NCSR maturity scoring compared to those not using a framework.

Response and Recovery Planning

23% responded “Not Performed” for the assessment question specific to having response plans and recovery plans in place. K-12 NCSR participants that are performing this activity, and/or have documented policies/procedures applicable to a response plan and a recovery plan, displayed 94% higher overall average NCSR maturity scoring than K-12 NCSR participants that are not performing these activities.

Cyber Reporting to Decision Makers

59% stated they provide periodic (at least annual) information risk, control, and security reporting to top-level decision-makers. Those who provided periodic cyber reporting to decision-makers displayed 52% higher overall average NCSR maturity scoring than those organizations that did not perform this activity.

Maturity Findings of the K-12 Sector

The Nationwide Cybersecurity Review (NCSR) is a voluntary, annual self-assessment designed to help organizations establish a baseline score of their cybersecurity maturity, on a scale of 1 through 7, according to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). Numerous state and federal grant programs require completion of the NCSR to qualify for funding. The 2022 NCSR results highlighted numerous trends in K-12 cybersecurity maturity.

Overall

2022 saw the highest participation rate for K-12 organizations in the NCSR's 11-year history, with 402 members completing the assessment. The overall average maturity score of K-12 NCSR participants was 3.25, compared to last year's score of 3.55. The 2022 score, although slightly lower than the 2021 score and below local sectors like public utilities, health services, and election offices, still stands at a satisfactory level of "3."

High Maturity Categories

Areas where K-12 schools are generally performing well include:

Identity Management and Access Control	Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
Awareness and Training	Organizations' personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
Maintenance	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

In addition to Identity Management and Access Control and Awareness and Training retaining their top two positions from the 2021 NCSR, K-12 schools are also demonstrating improved performance in the Maintenance category when compared to last year's assessment, where Business Environment ranked as the third highest maturity category.

Low Maturity Categories

Areas where K-12 schools are generally performing poorly include:

	ASSOCIATED BEST PRACTICES TO IMPLEMENT	
NIST CSF Category	**CIS Critical Security Control**	**Recommended Actions**
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
	CIS Control 10: Malware Defenses	• Disable Autorun and Autoplay for Removable Media
Information Protection Processes and Procedures	**CIS Control 7:** Continuous Vulnerability Management	• Perform Automated Vulnerability Scans of Externally Exposed Enterprise Assets
Supply Chain Risk Management	**CIS Control 11:** Data Recovery	• Test Data Recovery
	CIS Control 15: Service Provider Management	• Monitor Service Providers
Detection Processes	**CIS Control 17:** Incident Response Management	• Designate Personnel to Manage Incident Handling • Establish and Maintain an Incident Response Process • Conduct Routine Incident Response Exercises • Conduct Post-Incident Reviews

These categories reflect the three NIST categories with the lowest maturity as reported by K-12 schools in the 2022 NCSR. These categories have been mapped to the corresponding CIS Critical Security Controls® (not presented in order of importance). While Protective Technologies and Supply Chain Risk Management remain as areas with low maturity scores for K-12 schools, they now also exhibit low maturity scores in Information Protection Processes & Procedures and Detection Processes, which were not reported as low-performing categories in the 2021 assessment. To ensure that you're meeting the minimum standard of security maturity, CIS recommends K-12 schools start with Implementation Group 1 (IG1) of the CIS Controls.

Ransomware Findings

Ransomware continues to be one of the top concerns for K-12 organizations, and it is essential for organizations to prepare and test for the efficacy of their incident response plans to limit the scope and impact before a full-blown attack.

What Happened?

During the 2022-2023 school year, a K-12 district was impacted by ransomware. They notified the MS-ISAC of the incident after receiving mixed results with the commercial vendor who initially was primary on incident response.

How Did the MS-ISAC Respond?

The MS-ISAC Security Operations Center (SOC) supporting MS-ISAC members took the initial incident report, collected incident details, and connected the member to the MS-ISAC Cyber Incident Response Team (CIRT). After scoping the incident on an initial incident response call, CIRT provided guidance and tools to the member to collect forensic artifacts and logs. This included artifacts and logs from the affected domain and configuration servers, which helped to better assess the threat actor's actions and establish indicators of compromise (IOCs). As part of interdepartmental MS-ISAC coordination, the MS-ISAC Cyber Threat Intelligence (CTI) team provided additional intelligence on the threat actor to assist CIRT's efforts. CIRT provided scripts to the impacted school district to determine where identified IOCs were present in their IT environment. Additionally, CIRT provided guidance to assist with the recovery effort and identified the threat actor's ransomware binary that was used to encrypt files. All this work led to establishing a timeline of events going from initial access to data exfiltration and encryption.

What Was the Impact?

The MS-ISAC response by SOC, CIRT, and CTI teams provided the affected school district with timely assistance. As a result, the school district better understood how to identify and investigate the threat activity. The district indicated that the MS-ISAC response was instrumental in understanding the incident timeline, developing IOCs, and obtaining necessary guidance to help restore the network. They were especially appreciative for the "above and beyond" efforts that the CIRT provided to help restore access to school enterprise systems during a busy school year.

Here are some actions you can take today to reduce the risk and impact from ransomware:

Prioritize and remediate known exploited vulnerabilities

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—the Cybersecurity and Infrastructure Security Agency (CISA) maintains the authoritative source of vulnerabilities that have been exploited in the wild: the **Known Exploited Vulnerability (KEV) catalog**.

The KEV catalog sends a clear message to all organizations to prioritize remediation efforts on the subset of vulnerabilities that are causing immediate harm based on adversary activity. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.

Train users to recognize and report phishing attempts

Teach employees to keep their guard up on all communications platforms, including social media, and flag suspicious correspondence for security review.

Educate employees on what to do when they receive a phishing email—regardless of whether they fell for it.

Enable and enforce multi-factor authentication

Require phishing-resistant multi-factor authentication (MFA) for all services to the extent possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems.

Incident Response

We recommend that K-12 schools have an incident response (IR) plan in place when a cyber risk is detected. The primary goal of IR is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. One crucial aspect of incident response planning is making sure your plans can be efficiently executed when an incident occurs. Partners in need of assistance with incident planning can join the Business Resiliency Working Group and later become members of our Incident Response Planning and Operations Workbench community.

To help develop an IR plan, K-12 organizations can use tabletop exercises to consider different risk scenarios, prepare for potential cyber threats, and identify tactical strategies for securing their systems. Tabletop exercises are designed to help organizations consider different risk scenarios and prepare for potential cyber threats. All the exercises can be completed in as little as 15 minutes, making them a convenient tool for putting your team in the cybersecurity mindset. In addition, each scenario will list the processes being tested, threat actors identified, as well as the impacted assets.

The incident response process consists of four steps: Plan, Detect, Respond, and Update.

Plan

Develop documentation for all procedures necessary to handle an incident.

Detect

Monitor enterprise assets and analyze intelligence to understand if an incident has occurred.

Respond

Activate the incident response plan to deal with an incident.

Update

Understand which portions of the incident response plan have been effective and update the plan accordingly.

K-12 organizations can report incidents by calling the CIS SOC at 866-878-4722 or emailing soc@cisecurity.org.

Additionally, CIS and CoSN have developed the K-12 Cybersecurity Incident Response Steps that outline the actions K-12 organizations can take before and during a cybersecurity incident.

Who you should call when a cyber incident strikes

Law Enforcement

It's important to inform appropriate law enforcement authorities at the outset of a cyber incident.

Cyber Insurance

Cyber insurance companies may have stipulations guiding your initial actions in the event of a cyber incident.

CIS SOC

The CIS Security Operations Center (SOC) regularly supports public sector organizations during cyber incidents, providing initial recommendations, analyzing indicators of compromise (IOCs), and assisting with mitigation.

Industry-specific Contacts

Organizations in certain industries may have specific notification requirements when experiencing a cyber incident.

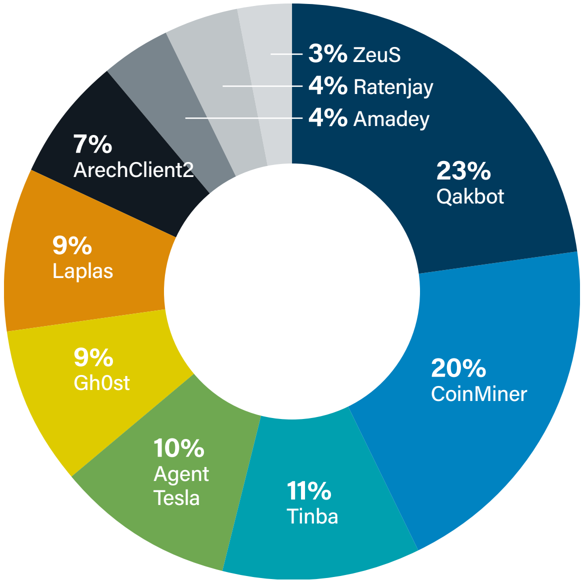
Internal Contacts

Following your incident response plan should involve notifying appropriate leaders and individuals in your organization of a cyber incident.

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 August 2022 through May 2023, Qakbot and CoinMiner were the top two malware affecting K-12 entities, making up 43% of the Top 10 Malware. This contrasts with the prior year's assessment when Shlayer, a type of malware that targets Apple macOS, posed the most significant threat to K-12 entities.



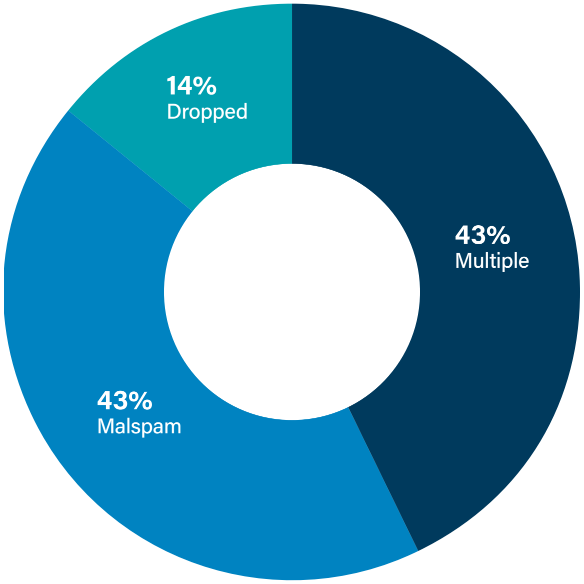
QakBot is a versatile banking Trojan with a wide range of capabilities, including enumeration (using commands like net, whoami, nslookup, netstat, ipconfig, etc.), lateral movement through SMB, keylogging to steal user credentials, network traffic monitoring, and the ability to deploy additional malware. Specifically, it targets online banking websites using a Man-in-the-Middle (MitM) technique to intercept authentication tokens during active banking sessions. QakBot can also load various modules, including credential and cookie harvesters, a Virtual Network Computing (VNC) module, Cobalt Strike, and an email collection module. Furthermore, it can lead to other malware infections, such as ransomware. After its operators are done with an infected host or network, QakBot uses Cobalt Strike modules to sell or grant access to other cyber threat actor (CTA) groups. It spreads primarily through malspam, often involving thread hijacking.

CoinMiner, a cryptocurrency miner family, typically employs Windows Management Instrumentation (WMI) for network propagation. It frequently relies on WMI Standard Event Consumer scripting for persistence, though its capabilities may vary due to multiple variants. CoinMiner is usually distributed through malspam or as a payload dropped by other malware.

Tinba, also known as Tiny Banker, is a banking Trojan distinguished by its compact file size. It uses web injections to capture victim information from login pages and web forms and is primarily disseminated through exploit kits.

From August 2022 through May 2023, Qakbot and CoinMiner were the top two malware affecting K-12 entities, making up 43% of the Top 10 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.

43%

Multiple

Malware that currently favors at least two vectors, such as Dropped and Malspam.

43%

Malspam

Unsolicited emails that either direct users to malicious websites or trick users into downloading or opening malware. Agent Tesla, Kovter, and NanoCore are using this technique.

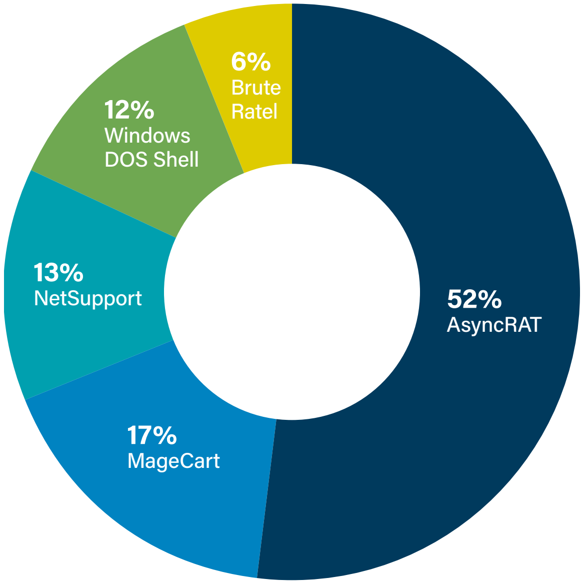
14%

Dropped

Data from Albert Network Monitoring and Management revealed that, from August 2022 to May 2023, Multiple, Malspam, and Dropped remained prominent initial infection vectors. In contrast, Malvertisement dropped out of the top 10, likely due to Shlayer being the only malware using this technique, and Shlayer is no longer a significant threat to K-12 schools during this period.

Top 5 K-12 Non-Malware Threats

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.



From August 2022 through May 2023, exploitation activity—the top two non-malware threats affecting K-12 entities were AsyncRAT and MageCart, making up 69% of the Top 5 Non-Malware threats observed by K-12 entities over that time. Interestingly, the Top 5 Non-Malware Threats in last year's MS-ISAC K-12 Cybersecurity Report have been supplanted this year by an entirely new set of threats. Changes in the Top 5 Non-Malware Threats from year to year occur for many reasons, most commonly due to the changing threat landscape, as well as CTAs continuing to evolve their tactics, techniques, and procedures (TTPs), abandoning TTPs that are no longer effective and employing TTPs that have a greater probability of achieving their goals.

AsyncRAT is an open-source Windows remote administration tool used for remote monitoring and control of computers via a secure encrypted connection. It is frequently misused with features like screen recording, keylogging, and remote desktop control, typically delivered through phishing, malvertising, and exploit kits.

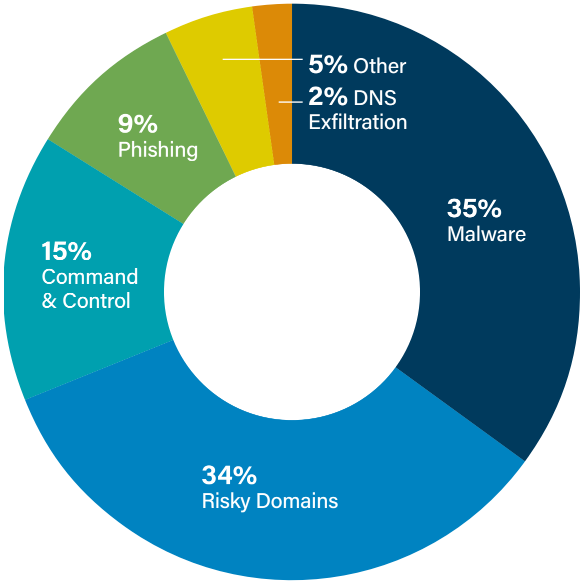
MageCart is a credit card skimming script that steals payment data from vulnerable website forms. Traffic to this domain suggests potential compromise of sensitive financial data on the affected host.

NetSupport is a remote access tool originally designed for providing technical support or computer assistance but is often exploited for malicious purposes, thanks to its remote desktop control capabilities and other features.

Three of the Top 5 Non-Malware Threats are legitimate tools, making up 72% of Top 5 Non-Malware Threat activity. AsyncRAT and NetSupport were the first and third respectively in this year's Top 5 Non-Malware Threats, making up 65% of the Top 5 non-malware activity. Both are legitimate remote access tools used for remote technical support or computer assistance. The third legitimate tool in the Top 5 Non-Malware is Brue Ratel, a tool used by security analysts to conduct penetration testing.

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 August 2022 and May 2023, malware still ranked as the most blocked activity in MDBR, but there is a 25% decrease in K-12 schools reporting it as a trend compared to the 2022 K-12 Report.

CoSN EdTech Survey

CIS is proud to partner with the Consortium for School Networking (CoSN). CoSN provides thought leadership resources, community, best practices, and advocacy tools to help leaders succeed in digital transformation. CoSN currently represents more than 13 million students. Each year, CoSN conducts a survey to provide a national perspective on the EdTech landscape, the challenges EdTech Leaders face, and the successes they've had.

For a decade, CoSN has been asking EdTech Leaders about their top priorities. Although the number of options provided in the survey has increased from 16 to 26, comparisons provide insight into just how much has changed over the years.

What has not changed in 10 years though is the struggle with insufficient resources. Budget constraints remain the number-one challenge facing EdTech Leaders. Although budgets have increased over the years, so have the IT areas that budgets must fund.

Pertinent to this report, the additional findings outlined below provide a window into the state of K-12 cybersecurity and how K-12 organizations are mitigating risks within the limitations of overly-constrained budgets:

Inadequate Funding

Inadequate funding is glaringly apparent for the 12% of districts reporting zero allocation in their district's IT budget for sustaining cybersecurity defense.

Since 2018, survey respondents have consistently identified cybersecurity as their number-one priority.

Cybersecurity Insurance

Year-Over-Year Comparison of Cyber Insurance Policy Purchases

POLICY PURCHASED	2023	2022
Yes, separate	**31%**	24%
Yes, umbrella	**43%**	38%
No	**11%**	19%
Planning	**3%**	3%
Not sure	**11%**	16%

Cybersecurity insurance is purchased by 89% of all districts, an increase from 81% the prior year. Umbrella policies are the most common type, which account for 43%. The remaining balance of districts (31%) purchase cyber insurance as a separate policy. Districts that do not purchase insurance account for 11%, down from 19% in 2022. The percentage of EdTech Leaders who are not sure if their district has a policy is also down year over year, down to 11% from the previous 16%.

This is an encouraging sign, as it suggests more EdTech Leaders are part of the cybersecurity insurance discussion in their districts. Increasingly, insurance companies have prerequisites for purchase and requirements for payout. EdTech Leaders need to know the details to ensure the district can comply.

Top 5 Recommendations for K-12 Organizations

1

Join the MS-ISAC to gain a valuable partner in your cyber defense

By joining the MS-ISAC K-12 Working Group, you can establish connections with similar organizations and contribute to enhancing the collective cybersecurity stance of the community. You can also engage in networking and collaborative discussions with fellow cybersecurity experts within the CIS WorkBench Community, where you can share and learn about best practices for securing the technologies you rely on.

2

Complete the NCSR to gauge your cyber maturity

Haven't completely the NCSR yet? Request information about the abbreviated Foundational Assessment at foundationalassessment@cisecurity.org. The 32-question Foundational Assessment is for organizations looking to assess their cybersecurity programs but have not yet taken the more comprehensive NCSR.

3

Complete Implementation Group 1 (IG1) of the CIS Critical Security Controls

Protect your organization with globally-recognized cybersecurity best practices by claiming your no-cost CIS SecureSuite Membership to chart and guide your path toward IG1 implementation, which has proven to be between 77% and 86% effective at defending against common cyber attacks.

4

Sign up for the MS-ISAC Indicator Sharing Program

Receive near real-time cyber threat intelligence you can act on.

5

Implement an intrusion detection system (IDS) and endpoint detection and response (EDR)

Learn how to protect your IT environment with Albert Network Monitoring and Management and Endpoint Security Services (ESS) solutions offered by CIS to see if they are right for your organization.

Services Available to MS-ISAC Members

MS-ISAC membership is available at no-cost to all U.S. State, Local, Tribal, and Territorial (SLTT) government organizations. Members benefit from numerous no- and low-cost services and resources to help build and maintain effective cybersecurity programs.

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		✓

Services Available to MS-ISAC Members (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		✓

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, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit www.CISecurity.org.

About the MS-ISAC

The Multi-State Information Sharing and Analysis Center® (MS-ISAC®) has been designated by the Cybersecurity & Infrastructure Security Agency (CISA) as the key resource for cyber threat prevention, protection, response, and recovery for all U.S. State, Local, Tribal, and Territorial (SLTT) governments. The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's SLTT governments through coordination, collaboration, cooperation, and increased communication. The MS-ISAC is a division of the Center for Internet Security® (CIS®), a 501(c)(3) nonprofit. Visit www.cisecurity.org/ms-isac/ or email info@msisac.org for more information.

About CoSN

CoSN is the premier professional association for K-12 EdTech leaders, their teams, and other school district leaders. CoSN provides thought leadership resources, community, best practices, and advocacy tools to help leaders succeed at digital transformation. CoSN represents over 13 million students and continues to grow as a powerful and influential voice in K-12 education.

CoSN also provides opportunities for companies that support the K-12 EdTech community to participate as corporate members.

Acknowledgements

We extend our sincere gratitude to the dedicated teams at CIS who collectively contributed to the creation of this report. Their collaborative efforts spanned a wide range of critical tasks, from data collection and analysis to conducting polls and surveys, compiling data, writing, reviewing, designing, and much more.

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.

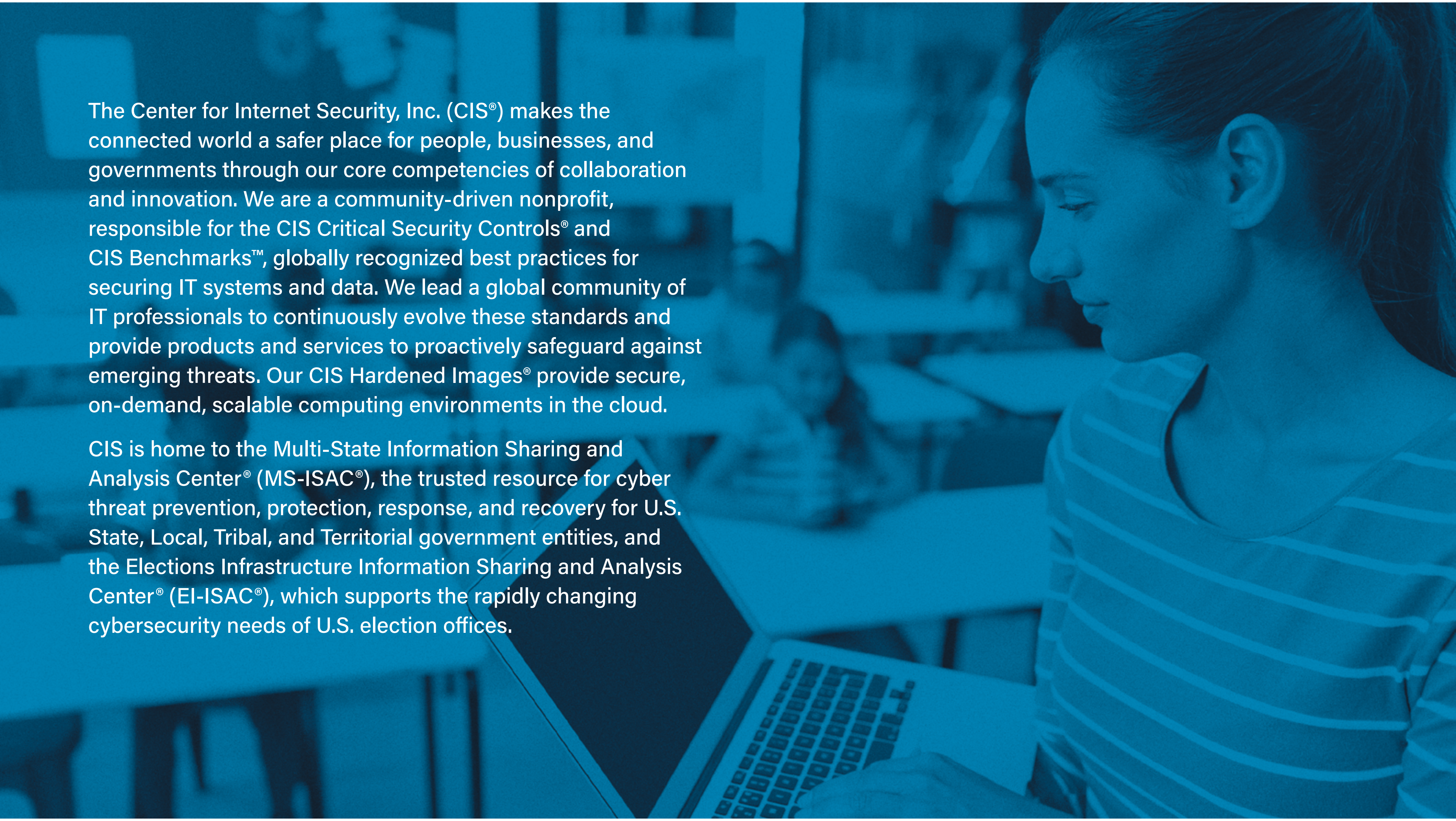
CIS Marketing and Communications Team: The Marketing and Communications Team played a pivotal role in crafting and conveying the message of this report, ensuring its clarity and reach.

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 understated. 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. Special thanks to the following individuals who went above and beyond to support this K-12 report: Scott Fosseen, John Wargo, Terry Loftus, Brad Hagg, and Bhargav Vyas.

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.



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, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices.

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