B26 - Cybersecurity: The Value of Shared Services in Defending School Districts

MSBO Annual Conference - 2026

plante moran | Audit. Tax. Consulting. Wealth Management. | 100 years

Introductions

Kyle Miller | Principal | Plante Moran

Matt Lindner | Senior Manager | Plante Moran

Today's talk

Cybersecurity feasibility study

- Enhance cyber capabilities in districts in the region
- Explore the feasibility of the ISDs providing CISO and SOC services to their constituent districts in a shared services model
- Phase 2 explored detailed staffing models and implementation frameworks

Objectives
• Identify the demand for cybersecurity services in K-12 in the region
• Develop scope of service offerings
• Define cost, staffing and service delivery models
• Examine scalability

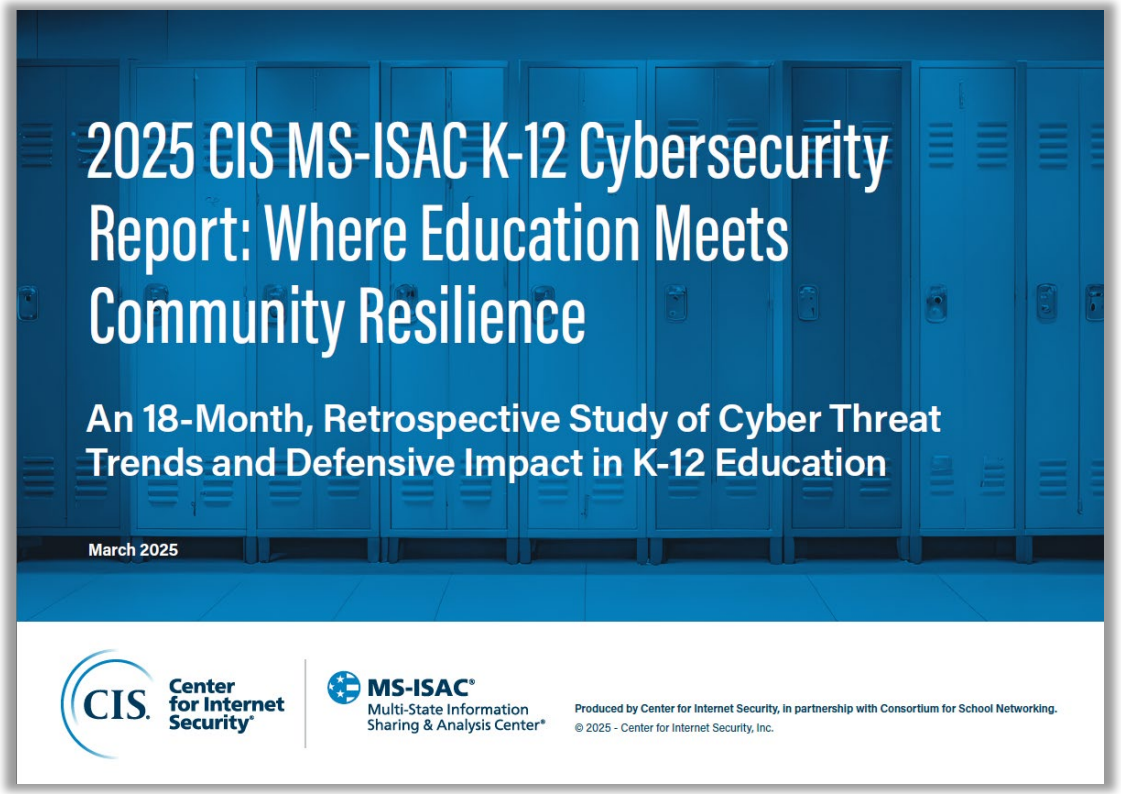
Kent consortium

- 3 Intermediate School Districts
- Kent ISD
- Muskegon Area ISD
- Ottawa Area ISD
- 43 local school districts | 35 charter schools
- Nearly 200,000 students

Feasibility study approach

Cyber risk to K-12

CIS MS-ISAC K-12 Cybersecurity Report



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 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

Top threats schools face

RANSOMWARE ATTACKS

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

MALVERTISEMENT

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

PHISHING AND SOCIAL ENGINEERING

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

DATA BREACHES

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

DENIAL-OF-SERVICE (DOS) ATTACKS

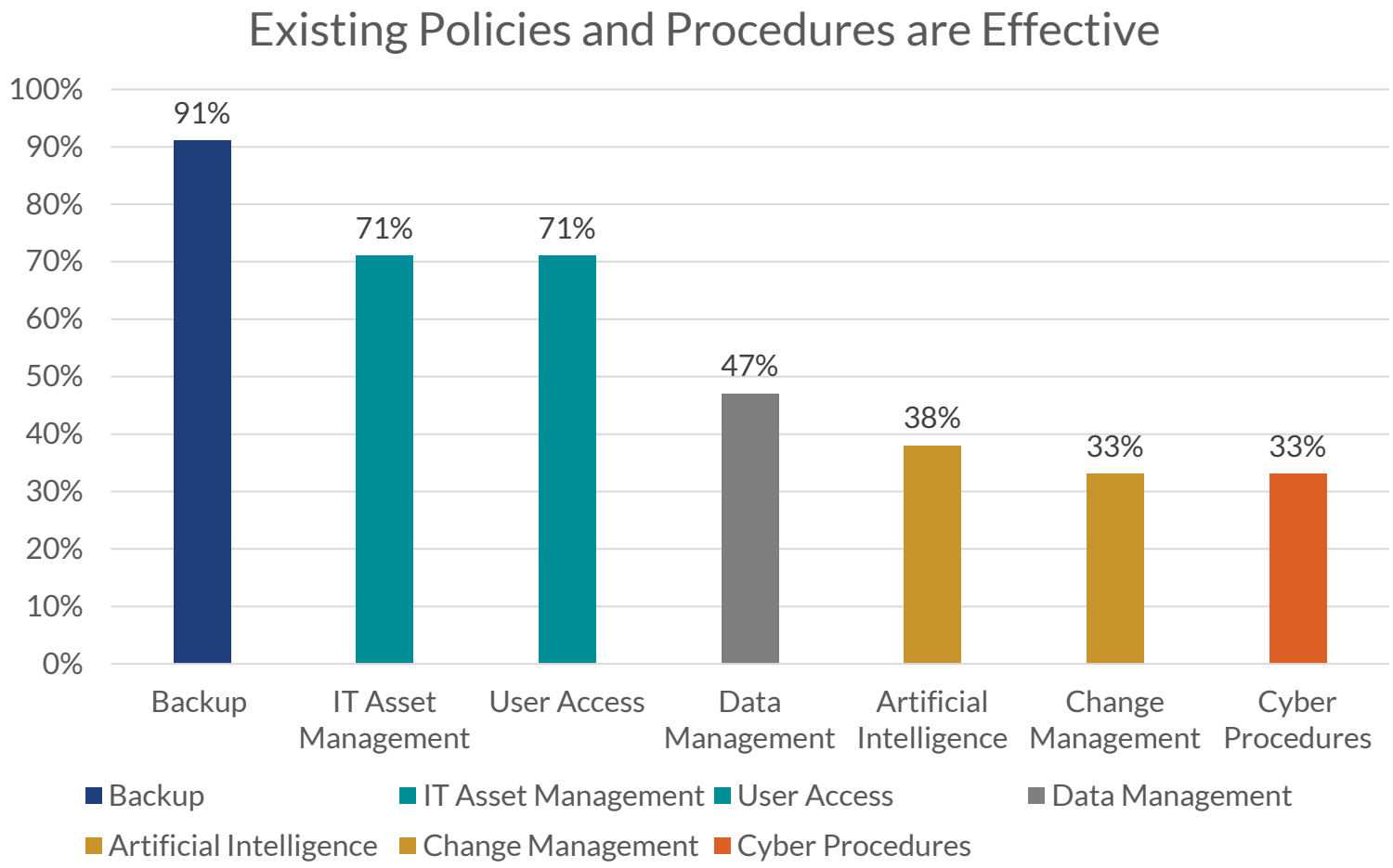
Cybercriminals overwhelm school networks, making online resources inaccessible.

Top 5 security concerns

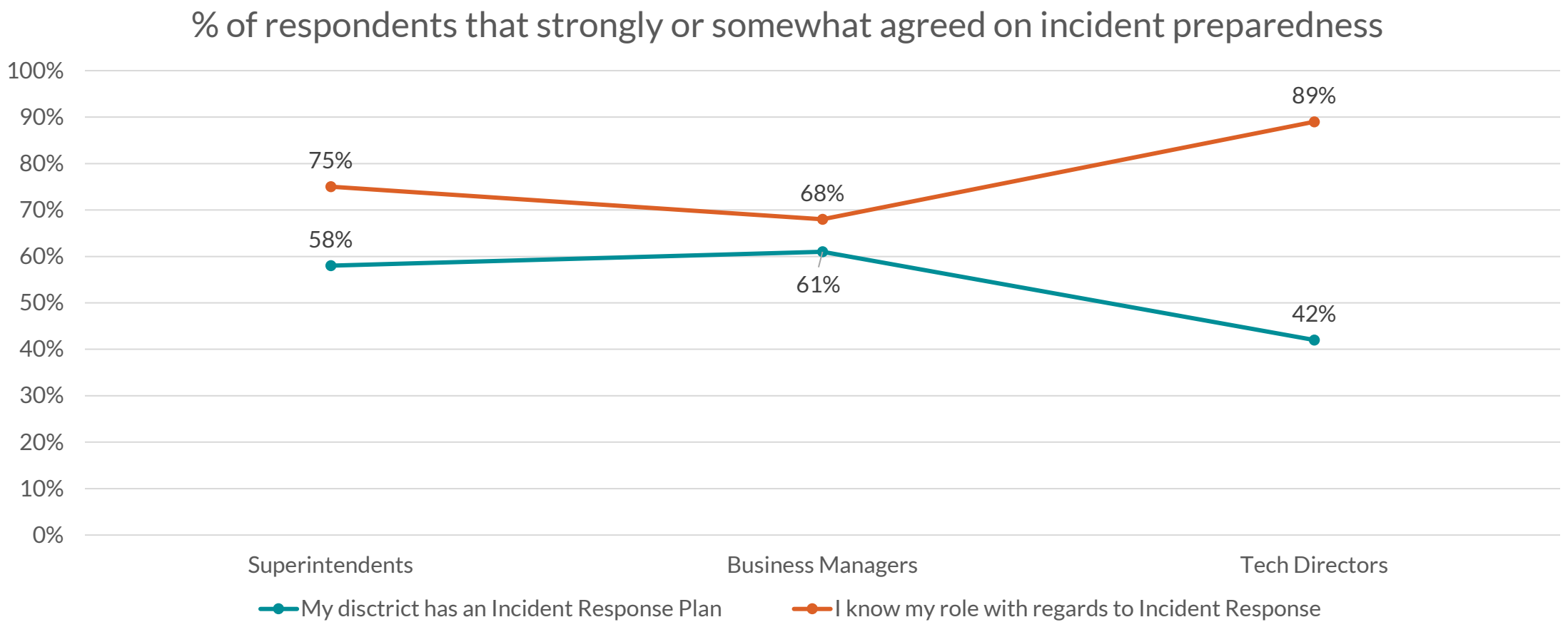
Top 5 Security Concerns	
Lack of Sufficient Funding	a. 86% of K-12 participants selected in the 2024 NCSR b. 82% of K-12 participants selected in the 2023 NCSR
Increasing Sophistication of Threats	a. 61% of K-12 participants selected in the 2024 NCSR b. 61% of K-12 participants selected in the 2023 NCSR
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

Updated feasibility study data

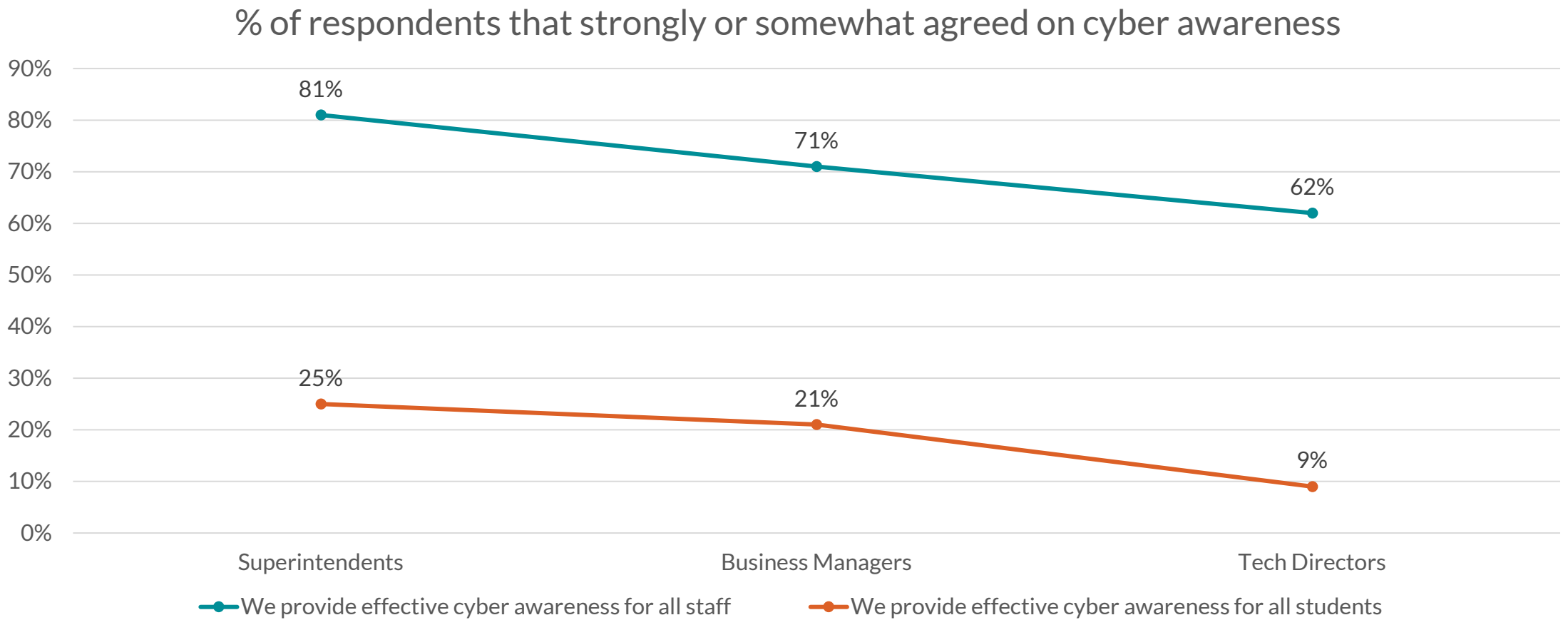
Policies & procedures



Incident preparedness



Cybersecurity awareness



Key Findings

And recommendations from CISA

FINDING 01

With finite resources, K–12 institutions can take a small number of steps to significantly reduce cybersecurity risk.

Key Recommendations:

- Implement highest priority security controls
- Prioritize CISA performance goals
- Develop a plan leveraging the NIST Cybersecurity Framework (CSF).

Cybersecurity maturity in K-12

Cybersecurity maturity according to the Nationwide Cybersecurity Review (NCRS)

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.

Cybersecurity high-points and low-points

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

FINDING 02

Many school districts struggle with insufficient IT resources and cybersecurity capacity.

Key Recommendations:

- Leverage funding opportunities
- Utilize free or low-cost services
- Expect strong security from IT providers
- Move to the cloud

Funding opportunities

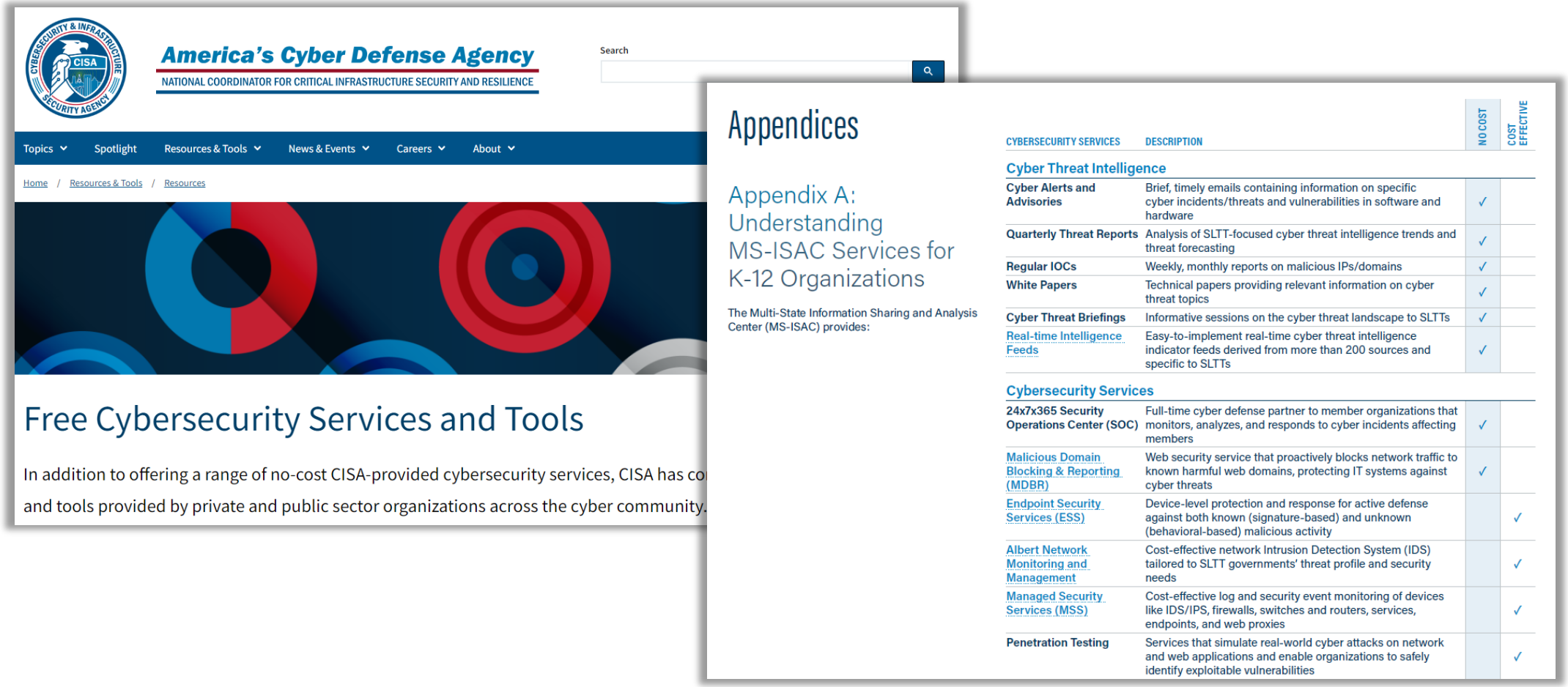
Michigan State and Local Cybersecurity Grant Program

- $2.35 million in funding in FY2025 to Michigan
- Annual application process TBD

FCC E-Rate Program

- FY26 cap of $5.2 billion
- Application based on highest level of poverty

Low-cost services



America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / Resources & Tools / Resources

Free Cybersecurity Services and Tools

In addition to offering a range of no-cost CISA-provided cybersecurity services, CISA has co
and tools provided by private and public sector organizations across the cyber community.

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		✓

FINDING 03

No K–12 entity can singlehandedly identify and prioritize emerging threats, vulnerabilities, and risks.

Key Recommendations:

- Join relevant collaboration groups & work with other information-sharing organizations
- Build a strong and enduring relationship with CISA and FBI regional cybersecurity personnel
- Explore potential shared services models

The value of collaboration

Some thoughts and findings on our study:

Established a framework for collaboration

- Consortium governance models
- Shared service delivery models
- Model for other collaboratives

Identified value and ROI

- Build vs. buy analysis
- Scalability considerations
- Procurement strategies

Service delivery framework

- Staffing strategies
- ‘Marketing’ to constituent districts
- CISO vs. SOC vs. Hybrid

The value of collaboration

Return on investment for local districts – CISO – Phase 1

CISO SERVICES COST AND POTENTIAL ROI					
	FTES REQUIRED	COST TO HIRE ONE FTE	DISTRICT SHARE OF ONE FTE	AVERAGE COST TO CONTRACT	ROI/COST AVOIDED
Small districts	.21	$228,648	**$48,016**	$70,800	$22,784
Medium districts	.26		**$59,448**	$150,606	$91,158
Large districts	.32		**$73,167**	$161,125	$87,958

The value of collaboration

Return on investment for local districts – CISO – Phase 2

CISO SERVICES COST AND POTENTIAL ROI				
TOTAL DISTRICTS	COST TO HIRE ALL FTES	DISTRICT SHARE	CONTRACT COST FOR ONE CISO PER DISTRICT	ROI/COST AVOIDED
5 Districts	$654,095	$130,819	$1,229,560	$575,465
10 Districts	$777,660	$77,066	$2.458,120	$1,680,460
15 Districts	$1,215,320	$81,021	$3,688,680	$2,473,360

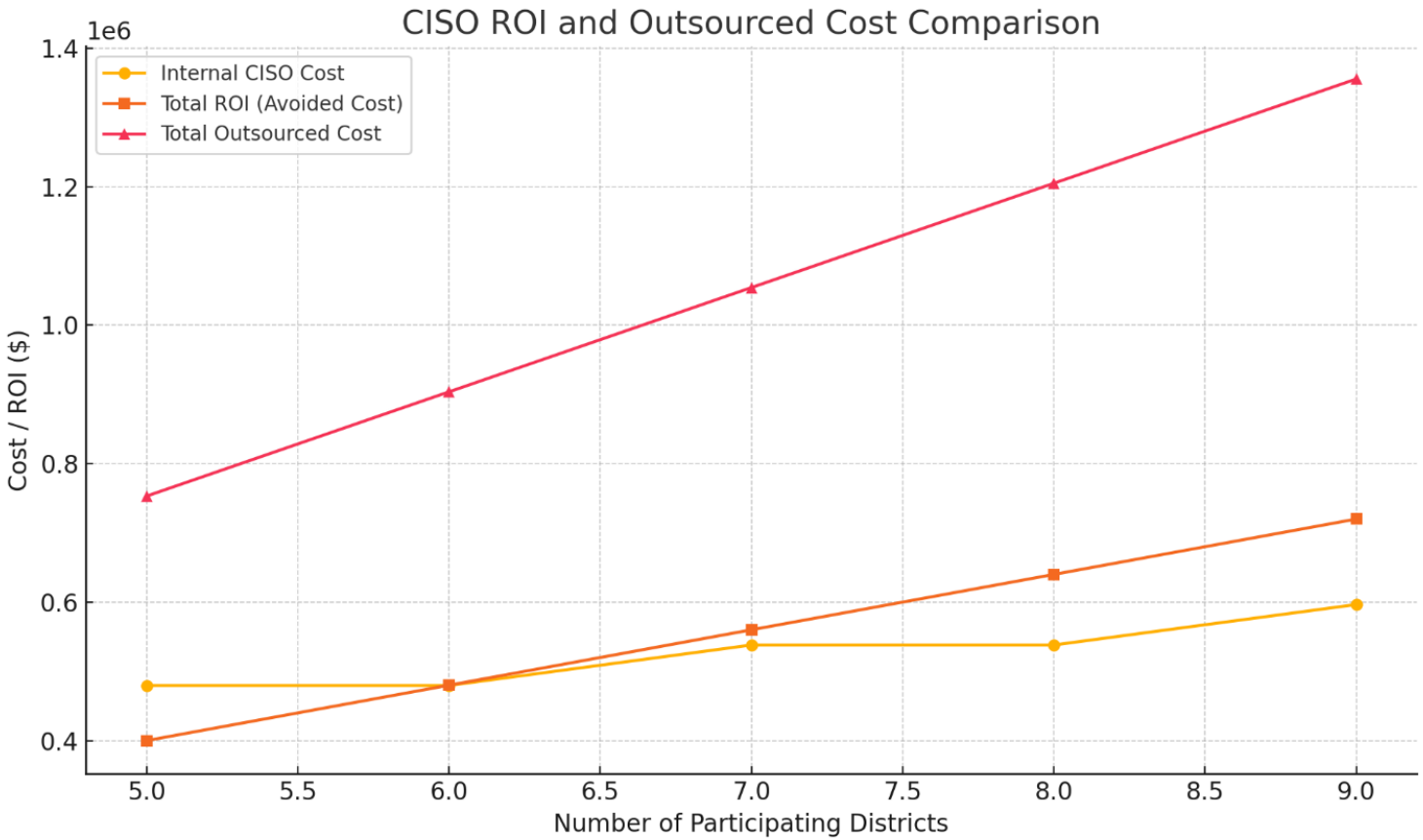
* Represents full program staffing costs for CISO, Managers and Specialists

The value of collaboration

Return on investment for local districts - SOC

SOC SERVICES COST AND POTENTIAL ROI CONSORTIUM MODEL/FULL PARTICIPATION						
	TOTAL TECH	FIXED LABOR	CONT.	TOTAL IMPL.	PER DISTRICT COST THRU ISD	ROI/COST AVOIDED
Small districts	$104,092	$166,900	$13,550	$284,542	$67,634	$216,908
Medium districts	$119,000		$14,295	$300,195	$82,541	$217,654
Large districts	$182,750		$17,483	$367,133	$146,291	$220,841

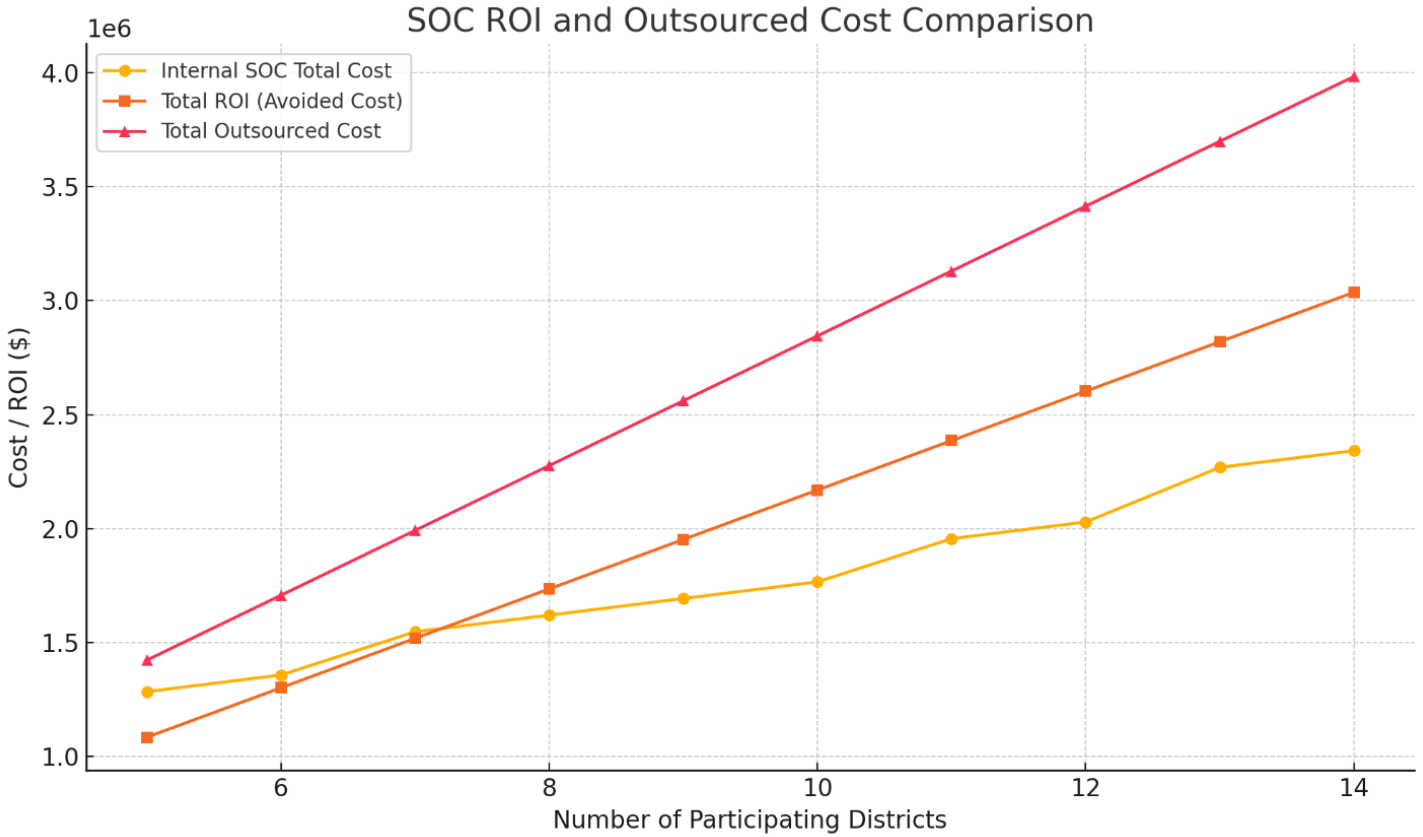
The value of collaboration



Return on investment for local districts – CISO Phase 2

* Represents full program staffing costs for CISO, Managers and Specialists

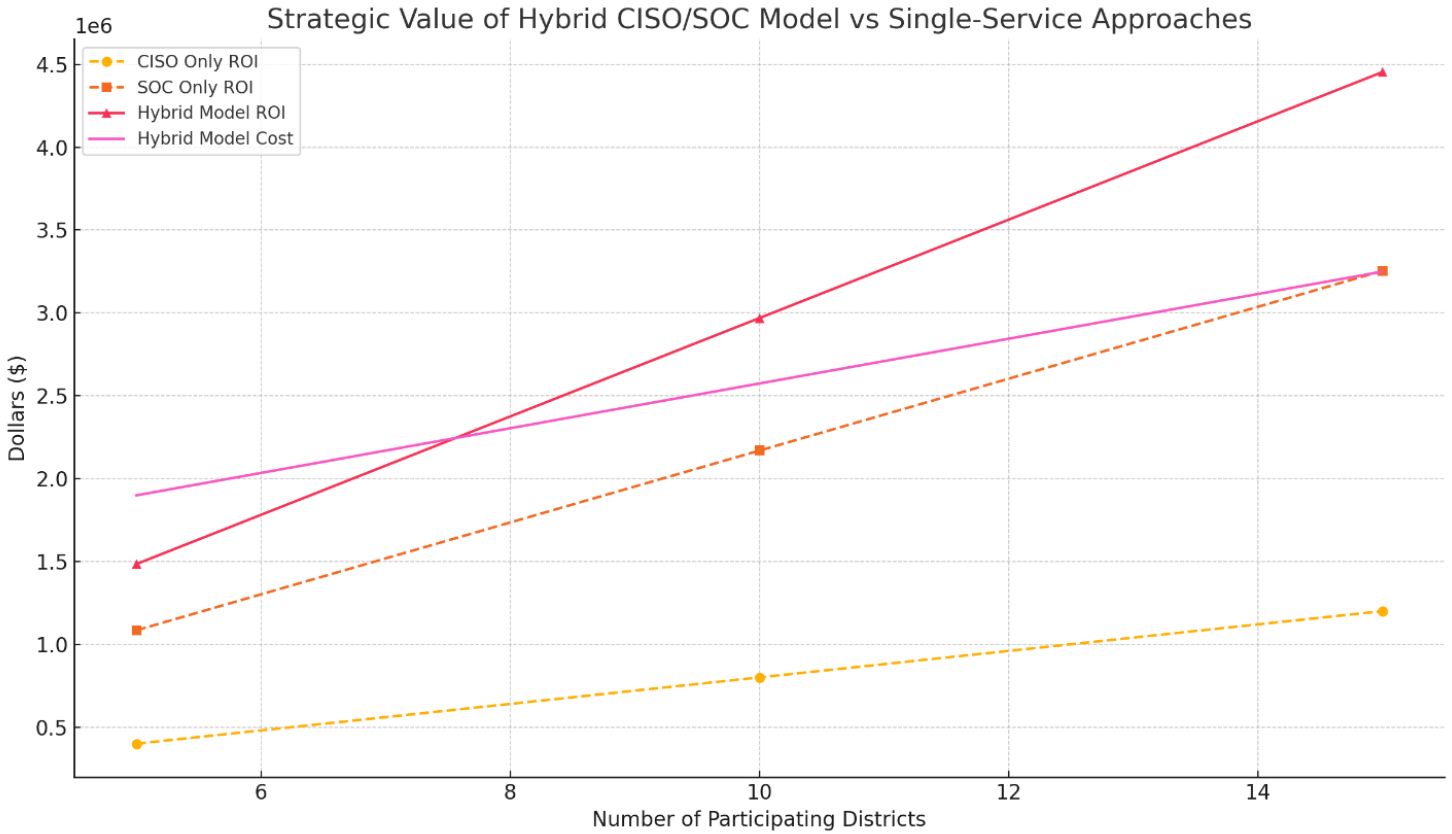
The value of collaboration



Return on investment for local districts – SOC Phase 2

* Represents full program costs for technology and staffing of CISO, Managers and Specialists

The value of collaboration



Return on investment for local districts – Hybrid Model - Phase 2

* Represents full program costs for technology and staffing of CISO, Managers and Specialists

Thank you!

Kyle Miller | CISSP, CISA, QSA, CDPSE

303-846-3518 | kyle.miller@plantemoran.com

Matt Lindner | ITIL, Agile CSM, Prosci CCP

248-223-3666 | matthew.lindner@plantemoran.com