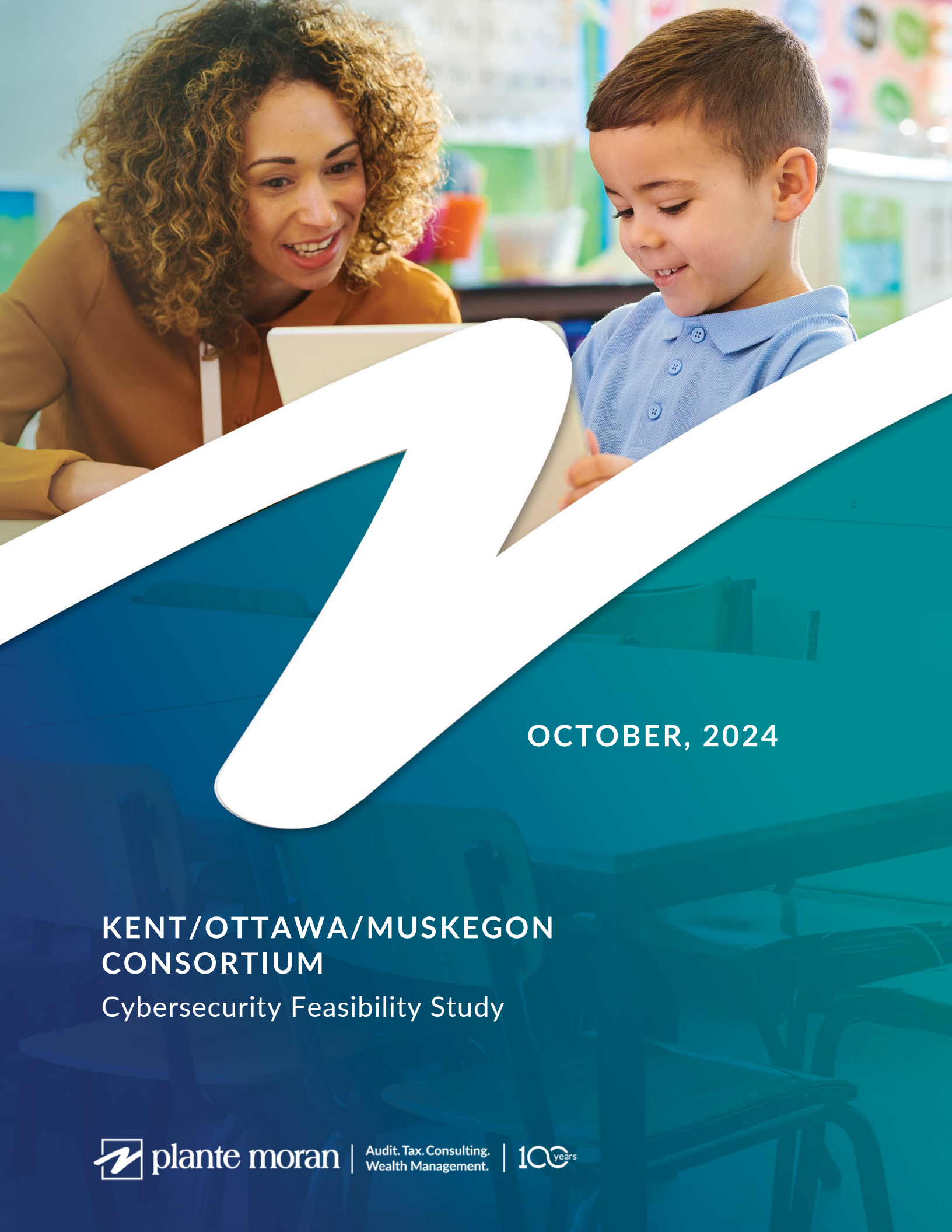




OCTOBER, 2024

KENT/OTTAWA/MUSKEGON CONSORTIUM

Cybersecurity Feasibility Study



plante moran

Audit. Tax. Consulting.
Wealth Management.

100 years

Contents

Executive summary	3
Project background	4
Project scope and methodology.....	5
Summary of findings and recommendations.....	8
Preliminary scope of services	10
Preliminary scope of services	11
ISD capability assessments.....	29
ISD capability assessments.....	30
Feasibility study	31
Feasibility study.....	32
Program recommendations	45
Appendix A: Glossary of acronyms.....	49

Executive summary



Project background

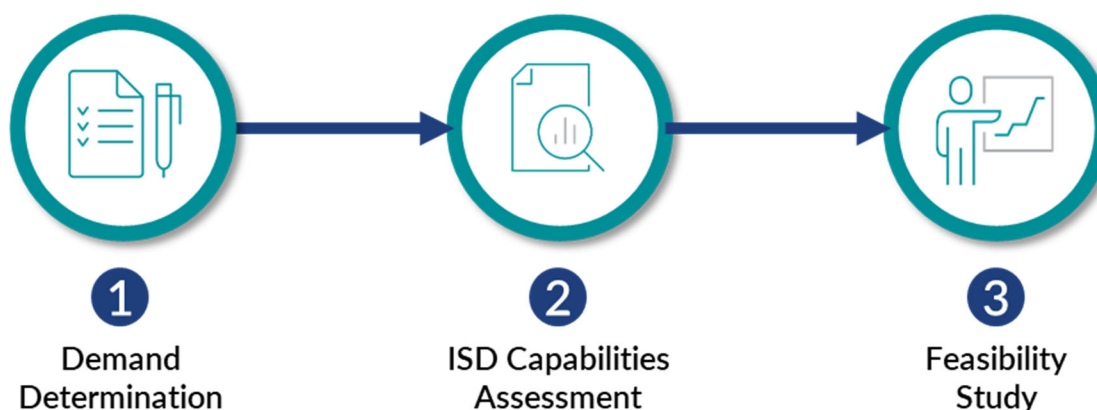
Kent Intermediate School District (Kent ISD), in collaboration with the Ottawa Area and Muskegon Area Intermediate School Districts, engaged Plante Moran to conduct a study to examine the feasibility of offering additional cybersecurity services to the local school districts and charter schools within their respective service regions. With the understanding that public education is a top target for cybercriminals and that public schools very often do not have the resources (both people and technical) to adequately secure their environments, the goal of this study is to:

- Identify the demand for cybersecurity services
- Develop a specific scope of potential services to be offered
- Examine staffing models for potential service offerings
- Define cost models for potential service offerings:
 - Costs to the Intermediate School Districts (ISDs)
 - Return on investment for local districts and charter schools
- Understand potential scalability within the region

Upon analyzing the information gathered through this study, Plante Moran was able to develop the conclusions and recommendations identified below.

Project scope and methodology

Our approach to this project included three major phases which were designed to identify a scope for potential service offerings and then examine the feasibility of developing and implementing those services.



Working with the ISDs, we conducted project initiation activities which included the formation of a project Steering Committee consisting of representatives from each ISD, as well as from a local school district within each of the three service regions in scope. Steering Committee membership for this study was as follows:

ORGANIZATION	MEMBER
Kent ISD	Glen Finkel – Assistant Superintendent of Technology Services Ryan Kelley – Region 1 Technology Lead
Muskegon Area ISD	Jeff Fielstra – Director of Technology Services Myles Sylva – Network Engineer
Ottawa Area ISD	Mike Rohwer – Chief Information Officer Rex Thelen – Chief Technology Officer
Fruitport Community Schools	Kevin Nielsen – Director of Technology
Grand Haven Area Public Schools	Michael MacDonald – Executive Director of Business Services
Lowell Area Schools	Nate Fowler – Superintendent

Detailed activities included within each phase of this study were as follows.

Phase 1: Demand determination

The goal for this phase was to understand existing cybersecurity capabilities among the local school districts and charter schools and gauge the level of demand for cybersecurity services from the ISDs. This phase also sought to identify the scope of potential service offerings prior to proceeding with the feasibility portion of the study.

We developed a series of surveys, which were administered to all superintendents, business managers, and technology directors within the three service areas in the scope of this study (Kent, Ottawa, and Muskegon). A summary analysis of survey responses is provided later in this study. Survey content included the following:

- Topics for all stakeholder groups:
 - Cybersecurity awareness
 - Incidents and incident response
 - Demand for cybersecurity services
- Role-specific topics:
 - Superintendents: Cybersecurity posture
 - Business managers: Cybersecurity planning and budgeting
 - Technology directors: Cybersecurity capabilities, policies, and procedures

We then conducted a series of focus groups with stakeholders from each of the three service regions in the scope of this study. Separate sessions were held for superintendents, business managers and technology directors (or equivalent titles in each role), with nine total focus groups being conducted. Topics for discussion in these sessions centered on the following:

- Existing capabilities at local districts and charter schools by individual chief information security officer (CISO) and security operations center (SOC) scope components
- Perceived need for services from the ISDs
- Considerations for staffing, governance, and service delivery
- Other considerations as brought up by participants

Upon completion of our analysis of the survey responses and information gathered via the focus groups, we developed a preliminary scope of services for CISO and SOC. This scope was presented to the Steering Committee for feedback prior to proceeding with subsequent phases of the project.

Phase 2: ISD capabilities assessments

The goal of this phase of the project was to understand existing capabilities at each ISD in the areas identified in the preliminary scope of services, and to determine their capacity to provide additional services from within their existing teams.

To gain a baseline understanding of each ISD's organization and operations, we requested and reviewed key existing documentation for initial discovery. Documentation reviewed included:

- Information security policies and procedures
- IT strategic plans
- Organizational charts
- IT and cybersecurity job descriptions
- Listings of IT systems and solutions
- Listing of critical technology vendor partners
- Security awareness training programs
- Cybersecurity insurance policies
- Cybersecurity-related budget information
- Results of any recent cybersecurity assessments

On completion of our review of the documentation provided, we conducted a series of interviews at each ISD to further our understanding of their capabilities. The result of this phase was a comparative assessment of the ISDs' capabilities which was then used to inform the subsequent staffing and delivery model for service offerings.

Phase 3: Feasibility study

To assess the feasibility of the ISDs providing CISO and SOC services, we developed assumptions and cost models around the following:

- Local district profile assumptions for small, medium, and large districts, including staff counts and technology endpoints
- Annual effort required to provide CISO services to a district of each profile
- Total compensation required to staff CISO and SOC services based on industry data in West Michigan
- Costs to implement the technologies required to provide SOC services

We also issued a Request for Information (RFI) to understand budgetary costs if the ISDs were to outsource these services to a managed services provider. This allowed us to perform a 'build versus buy' analysis for the services in scope for the programs. We additionally met with two major insurance carriers to understand the increased liability exposure that would result from these programs and coverage options to mitigate that risk. Finally, through an analysis of the data compiled, we developed cost and pricing models, as well as recommendations related to service delivery.

Summary of findings and recommendations

The discovery activities conducted through this study produced the following summarized findings. Note that more detail is provided for each later in this study:

KEY OBSERVATIONS

DEMAND

- Stakeholders who participated in surveys and focus groups consistently indicated that a demand for cybersecurity services exists within K-12.
- Many participants were aware of the need for greater security, but often their districts lacked the expertise or resources to meet all their needs.
- There is, however, a level of cost sensitivity related to any services the ISDs may provide, again given the lack of resources.

SCOPE OF SERVICES

- The majority of potential scope items were of interest to stakeholders, with a few limited exceptions.
- A desire for a-la-carte pricing was expressed but was determined to present too many challenges to be feasible.

STAFFING MODEL

- The need for expertise in cybersecurity and the K-12 education industry for any resources providing services was seen as critical by stakeholders.
- The existing ISD teams will need to be augmented if these programs are to be implemented. While the current staff do possess cyber skillsets, a lack of capacity was indicated.
- While a preference for local resources was indicated by stakeholders, access to resources when needed was a more critical concern.

BUILD VERSUS BUY

- Services contemplated in this study can be contracted for from managed services providers.
- Outsourcing does not appear to be the most cost-effective strategy, although further investigation is likely needed to confirm this at scale.

SUMMARY RECOMMENDATIONS

SCOPE OF SERVICES

- CISO services are recommended to include scope for cybersecurity strategy, incident readiness and response, and training and awareness.
- SOC services are recommended to include user and device management, logging and monitoring, and assessment and threat intelligence.

SERVICE DELIVERY MODEL

- A consortium-based model for SOC services is recommended based on the cost efficiencies it presents. Individual SOC's in each ISD appear to be cost prohibitive.
- A formal governance structure should be developed to operate shared, consortium-based programs.
- Demand discussions with stakeholders should be revisited to review program costs and gauge potential participation levels.
- A staffing strategy should be developed for both CISO and SOC resources.
- A strategy for operational capacity for CISO resources will be needed to allow the programs to quickly scale when new districts onboard.
- Standard operating procedures for both CISO and SOC should be developed to govern operations and performance management.
- Further scalability options for SOC services should be investigated to drive down costs.
- Outsourcing options should be further investigated to understand the buying power of the consortium based on assumed participation levels.

COSTS

- CISO costs should be allocated evenly to program participants based on the level of effort required to support their district.
- SOC costs should be allocated as an even share of fixed costs across all participants, plus each district's variable costs for items such as MDR and vulnerability scanning solutions.

Preliminary scope of services



Preliminary scope of services

To define a preliminary scope of services for any potential offerings from the ISDs, the study sought to understand the demand for services among LEAs and PSAs within the service regions in question. This was done through direct feedback from key stakeholders and decision-makers, including superintendents, business managers, and technology directors. Their feedback was obtained via a series of surveys and focus group interviews.

1. Stakeholder surveys

We developed and administered a series of surveys which were released to the superintendents, business managers, and technology directors throughout Kent, Muskegon, and Ottawa counties. These surveys sought to build a preliminary understanding of the cybersecurity posture of the LEAs and PSAs in the region. Separate surveys were developed for each stakeholder group, with the following topics being explored with all groups:

QUESTIONS FOR ALL STAKEHOLDER GROUPS:		
SUPERINTENDENTS	BUSINESS MANAGERS	TECHNOLOGY DIRECTORS
Cybersecurity awareness - All staff are effectively trained in cybersecurity awareness. - All students are effectively trained in cybersecurity awareness.		
Incidents and incident response - Incidents occurred in the last 18 months. - Effectiveness of incident response plans. - Understanding of one's role in an incident response scenario.		
Cybersecurity services - Interest in understanding potential CISO scope. - Interest in engaging the ISDs for CISO services. - Interest in understanding potential SOC scope. - Interest in engaging the ISDs for SOC services.		

Additionally, several role-specific questions were explored with each stakeholder group:

ROLE-SPECIFIC QUESTIONS:

SUPERINTENDENTS

Cybersecurity posture

- 1. Prioritization of cybersecurity in planning processes.
- 2. Confidence in skillsets to implement cybersecurity programs.
- 3. Allocation of adequate budgets for cybersecurity needs.

BUSINESS MANAGERS

Cybersecurity planning and budgeting

- 1. Adequacy of planning and budgeting for cybersecurity.
- 2. Existence of a dedicated cybersecurity budget.
- 3. Leverage of outsourced services (ISDs and other third parties) to augment internal capabilities.
- 4. Compliance with expanding liability insurance requirements

TECHNOLOGY DIRECTORS

Cybersecurity capabilities

- 1. Existing staff skillsets.
- 2. Existence of dedicated cybersecurity staff resources (internal and outsourced).
- 3. Staff professional development related to cybersecurity.

Cybersecurity policies and procedures

- 1. Existence of effective cybersecurity policies (including AI, backups, change management, data management, IT asset management, and use access).
- 2. Existence of defined cybersecurity procedures.

Stakeholder survey response summary

Stakeholder surveys were administered to all LEAs and PSAs within the region with the following response rate.

SUPERINTENDENTS	BUSINESS MANAGERS	TECHNOLOGY DIRECTORS
35 total	41 total	25 total
1 partial	1 partial	2 partial

A summary of those responses by stakeholder group is as follows:

SUPERINTENDENT RESPONSES

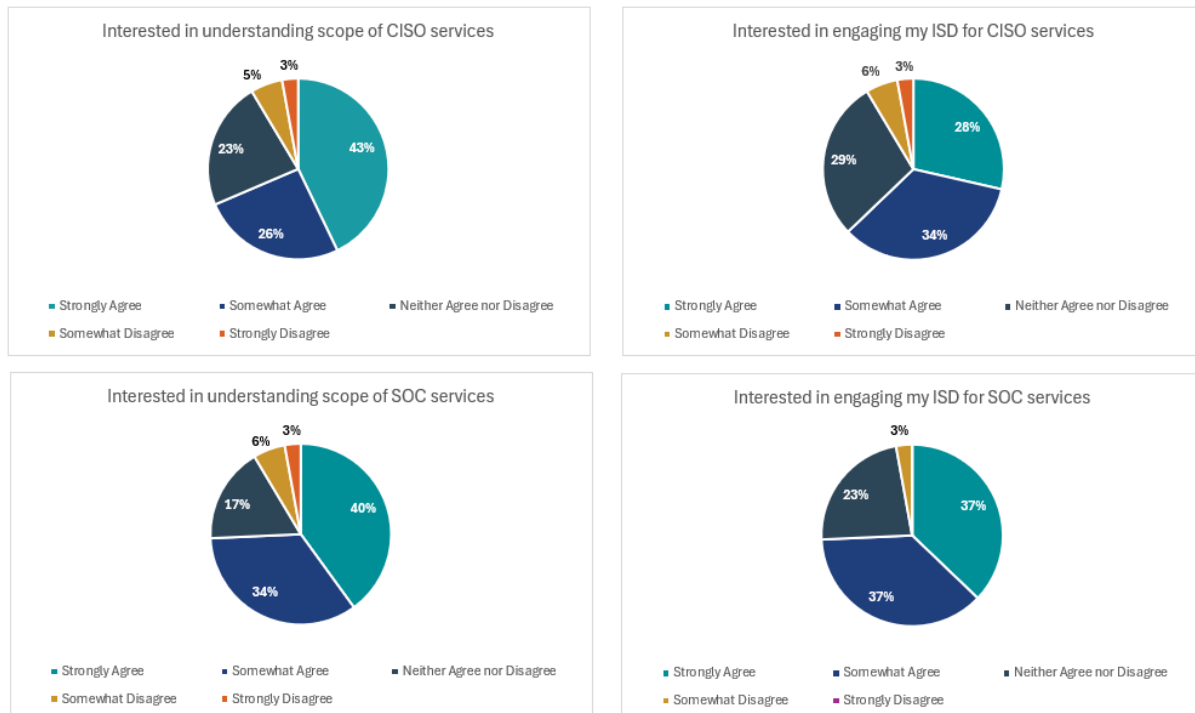
Cybersecurity posture: Superintendents who responded have a high degree of confidence in their district or charter school's cybersecurity posture:

- **91%** agree that cybersecurity is adequately prioritized in their district or charter school.
- **83%** agree that their staff has the requisite skillsets to effectively implement cybersecurity programs.
- **70%** agree that the necessary budget has been allotted for cybersecurity.

Cybersecurity awareness: Superintendents are confident in the awareness training provided to staff (**81%** feel that it is effective), but feel that opportunity exists to increase awareness among students (only **25%** feel that training for students is effective).

Incident response: Only **25%** of superintendents feel that their district/charter school has an effective incident response plan, while **75%** feel that they understand their role in an incident response scenario.

Interest in cybersecurity services: Superintendents who responded to the survey expressed significant interest in not only understanding the scope for cybersecurity services, but also in potentially engaging their ISDs for those services.



BUSINESS MANAGER RESPONSES

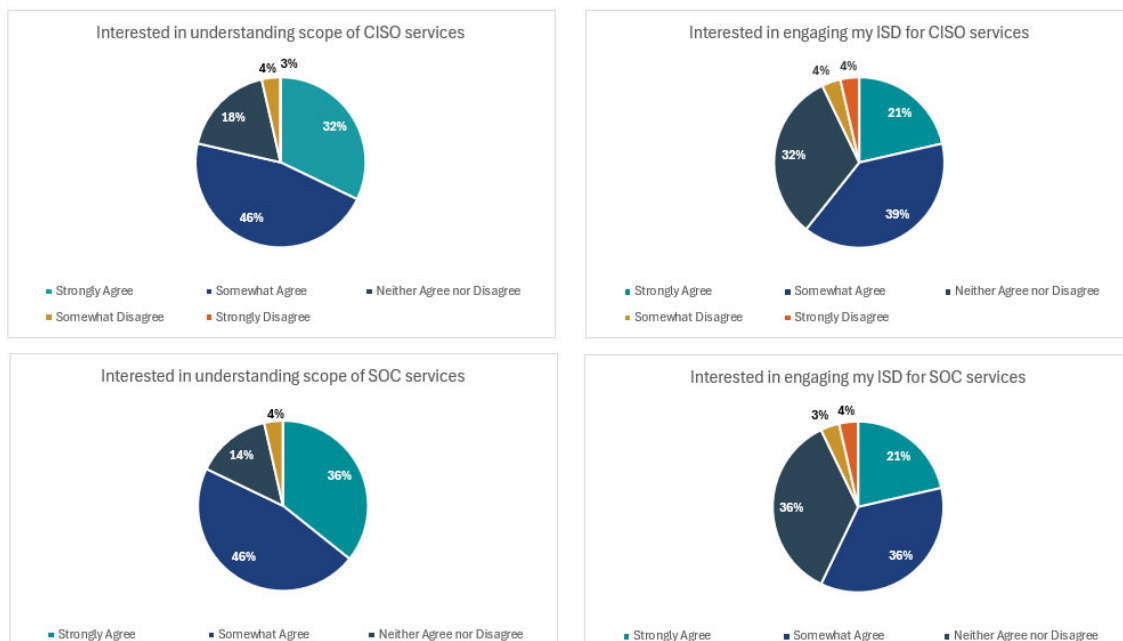
Cybersecurity planning and budgeting: Business managers who responded are reasonably confident that their district/charter school effectively leverages third-party providers (including the ISDs) and that they are able to maintain compliance with liability insurance cybersecurity requirements. They were also somewhat confident in the effectiveness of planning and budgeting activities that are undertaken.

- **68%** agree that cybersecurity is adequately planned and budgeted for in their district or charter school. It should be noted, however, that only **4%** of respondents indicated that they have a dedicated budget for cybersecurity.
- **86%** agree that their district or charter school effectively leverages third-party providers, including ISDs, for cybersecurity services.
- **75%** agree that they are able to maintain compliance with the cybersecurity requirements of their liability insurance provider.

Cybersecurity awareness: Much like their superintendents, business managers are confident in the awareness training provided to staff (**71%** feel that it is effective), but feel the opportunity exists to increase awareness among students (only **21%** feel that training for students is effective).

Incident response: Only **30%** of business managers feel that their district/charter school has an effective incident response plan, while **68%** feel that they understand their role in an incident response scenario.

Interest in cybersecurity services: Business managers who responded to the survey expressed interest in both understanding the scope for cybersecurity services, as well as potentially engaging their ISDs for those services. Note that this level of interest is somewhat less than that expressed by superintendents.



TECHNOLOGY DIRECTOR RESPONSES

Cybersecurity capabilities: Technology directors who responded are reasonably confident that they have the requisite skillsets in their teams to protect their district/charter school, and even more so that they can get their teams the training that they need. Very few have dedicated cybersecurity resources, either on their teams or via third-party providers:

- **71%** agree that their teams possess requisite cybersecurity skills.
- **82%** agree that they can get their staff the training that they need related to cybersecurity.
- **22%** have dedicated cybersecurity resources on their teams, while **36%** utilize third-party providers as dedicated cybersecurity resources.

Cybersecurity awareness: Technology directors are the least confident stakeholder population in regard to cybersecurity awareness. **62%** feel that staff training is effective, while only **9%** feel that student training is effective (or exists).

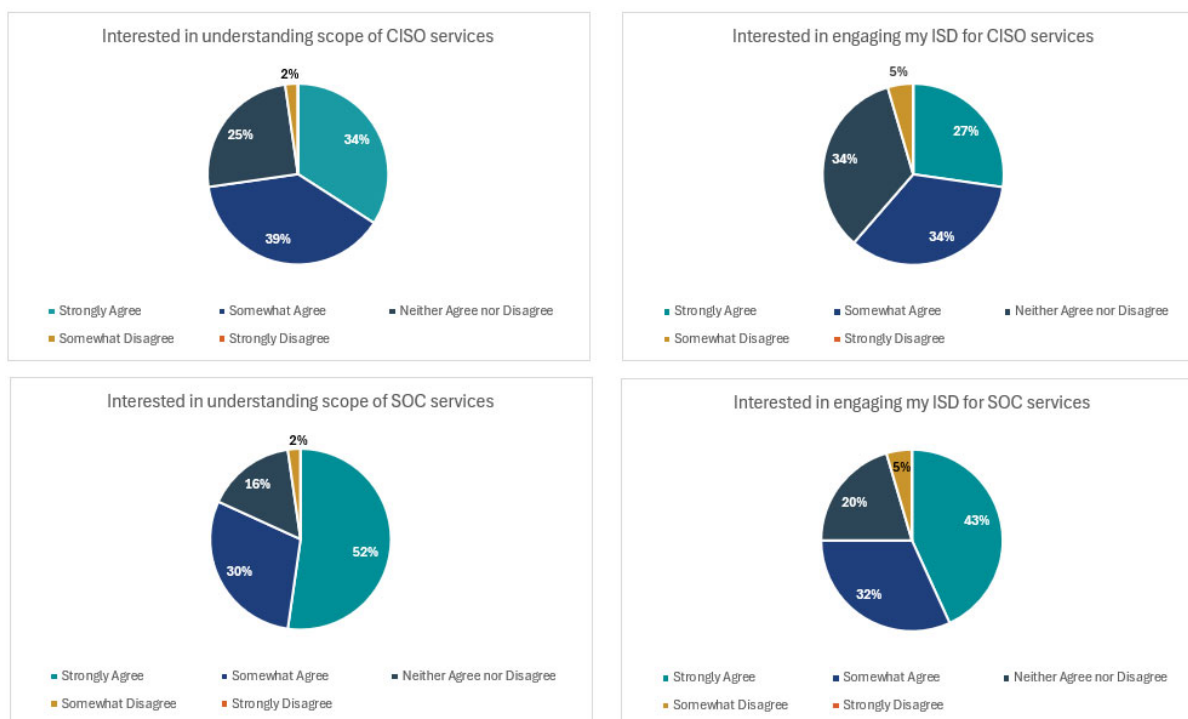
- When asked what initiatives are currently underway to foster awareness in their district/charter school, the most commonly used strategy was phishing tests (**84%**) followed by email or other communications campaigns (**73%**).
- Only **27%** of respondents were employing strategies other than those two options.

Incident response: Only **21%** of technology directors feel that their district/charter school has an effective incident response plan, while **89%** feel that they understand their role in an incident response scenario.

Cybersecurity policies and procedures: Technology directors who responded generally feel that deficiencies exist with regards to their cybersecurity related policies and procedures.

- **38%** agreed that they have adequate **artificial intelligence** related policies in place.
- **91%** feel that their **backup policies** were sufficient, by far the most positive response.
- **33%** indicated that they have strong **change management policies**.
- **47%** feel that they have strong **data management policies**.
- **71%** agreed that their **IT asset management** and **user access policies** were effective.
- Only **33%** of technology directors felt that their overall **cybersecurity related procedures** were adequately developed and defined.

Interest in cybersecurity services: Technology directors who responded to the survey expressed interest in both understanding the scope for cybersecurity services, as well as potentially engaging their ISDs for those services. Note that this level of interest is somewhat less than that expressed by superintendents and is more in line with the interest level of the business managers.



Overall, the survey results support the conclusion that there is demand for cybersecurity related services within the service region for this study. They also reveal several gaps in cybersecurity posture among the respondent population and highlight the need for augmented capabilities among the K-12 community.

These results were reviewed with the Steering Committee and used to inform the subsequent focus groups where more detailed discussions with stakeholders on these topics were possible.

Stakeholder focus groups

Following up and building on the data collected via the stakeholder surveys, we conducted a series of focus groups to facilitate more detailed discussions regarding the need for cybersecurity services among the LEA and PSA community within this study’s service region. We conducted sessions for superintendents, business managers, and technology directors within each county (nine total focus groups) to gather more detailed feedback on demand. The topics for these sessions primarily focused on the potential scope for services for CISO and SOC, the level of need for each scope component, and considerations for service delivery for those potential scope items. The following provides a summary of observations and feedback from the stakeholder focus groups:

SUPERINTENDENT FOCUS GROUPS

There were 18 total attendees across the three service regions participating in the superintendent focus groups.

ATTENDEES		
KENT ISD	MUSKEGON AREA ISD	OTTAWA AREA ISD
5 total districts	7 total districts	6 total districts

Superintendent scope feedback: CISO

- Strategy, planning, and budgeting was seen as an area of significant need/vulnerability, particularly given increased requirements from insurance carriers in this area.
- Risk assessments are an item on which the districts are already expending some resources/effort; however, there were questions regarding whether the current efforts are sufficiently comprehensive.
- Disaster recovery plan/continuity of operations plan development and testing is thought to be an ‘in progress’ item with most districts, with some level of plan development completed but limited testing done.
- Incident response plan development and testing is also thought to be somewhat inconsistently implemented and tested in most districts. Many participants indicated that they had begun the development of plans based on standard templates but had not completed development and had not done any testing.
- Cybersecurity insurance requirements are an area where districts thought they likely need the least assistance as they can currently maintain compliance. Some participants do anticipate a future need in this area as requirements continue to become more stringent.
- Staff development was seen as a priority, particularly in the area of end-user awareness training. This was an item that superintendents viewed as a high priority to be completed annually.

- Regulatory compliance (HIPAA, FERPA, and PCI) was viewed as a priority and an area of specific need, particularly as it relates to the proliferation of payment card transactions in districts.
- Vendor risk assessment and oversight is a growing priority as districts continue to leverage more third-party providers for a variety of services. The need for specific skillsets to evaluate capabilities and risks associated with vendor partners, as well as the ability to manage those partners effectively operationally, was seen as an area for opportunity to improve in many districts.
- Cybersecurity policy development was seen as an area of somewhat limited demand as many districts are leveraging their attorneys for the creation of these policies. However, if the opportunity was presented to provide these services more cost effectively, as well as to maintain policies on an ongoing basis, participants did see some level of opportunity/demand in this scope area.

Superintendent scope feedback: SOC

Discussions were held regarding the potential scope of services for SOC; however, given the technical nature of many of these items, the superintendents who participated in our focus groups tended to defer to their technology directors regarding the overall need/demand for individual scope components. When potential scope items (detailed in the list below) were discussed, the general sentiment was that while superintendents did see value in those items, they were unsure as to what was currently being done in those areas at their districts. Potential SOC scope:

- Penetration testing and vulnerability scanning
- Identity and access management
- Phishing assessments (this was an area where there was feedback, and it was generally stated that these assessments are already being done in most districts)
- Threat intelligence and identification
- Endpoint detection and response
- Log aggregation
- Mobile device management

Other feedback from superintendents

Superintendent participants provided additional feedback regarding service delivery and other considerations. The need for initial assessments from the ISDs, with resulting recommendations for services, was suggested. This would allow districts to focus their investment where the greatest value would be realized. As a component of this model, an a-la-carte model for services was proposed that would allow districts and charter schools to opt in for only those services that they desired. A need was also expressed for a level of ‘minimum services’ as recommended by the ISDs, as opposed to a full suite of SOC and CISO services. The general consensus among this group was the need for a consultative relationship that provided a level of flexibility and affordability to LEA and PSA participants.

The following is a snapshot of the level of demand indicated by participating superintendents for each potential scope component discussed.

- High (↑): Represents a high level of demand/services in this area are greatly needed
- Medium (▬): Represents a moderate level of demand/services in this area are somewhat needed
- Low (↓): Represents a low level of demand/services in this area are not needed

DEMAND FROM SUPERINTENDENTS			
CISO SERVICES		SOC SERVICES	
Strategy, planning, and budgeting	↑	Penetration testing and vulnerability scanning	Cannot rate
Risk assessment	↑	Identity and access management	Cannot rate
DRP/BIA development and testing	↑	Phishing assessments	Cannot rate
IRP development and testing	↑	Threat intelligence and identification	Cannot rate
Cybersecurity insurance compliance	↓	Endpoint detection and response	Cannot rate
Staff development	↑	Log aggregation	Cannot rate
Regulatory compliance	↑		
Vendor risk assessment and management	↑	Mobile device management	Cannot rate
Policy development	▬		

BUSINESS MANAGER FOCUS GROUPS

There were 17 total attendees across the three service regions participating in the business manager focus groups.

ATTENDEES		
KENT ISD	MUSKEGON AREA ISD	OTTAWA AREA ISD
4 total districts	7 total districts	6 total districts

Business manager scope feedback: CISO

- Strategy, planning, and budgeting was an area where the business managers saw a level of need; however, concern was expressed regarding the potential cost of services. Most participants indicated that their districts didn't have the excess funds they anticipated would be needed for these services, and highlighted the fact that they did not have dedicated budgets for cybersecurity services.
- Risk assessments are an item where greater interest was expressed, particularly if these assessments would enable a more strategic use of limited resources at their districts.
- Disaster recovery plan/continuity of operations plan development and testing is thought to be an 'in progress' item with most districts, with some level of plan development completed but limited testing done. Business managers' feedback was consistent with that of the superintendents in this area.
- Incident response plan development and testing is another area where the business managers echoed the feedback of the superintendents in that this is also thought to be somewhat inconsistently implemented and tested in most districts. Many participants indicated that they had begun development of plans based on standard templates but had not completed development and had not done any testing.
- Cybersecurity insurance requirements are an area where districts thought they likely need the least assistance as they can currently maintain compliance. One potential area for demand was operationally maintaining a level of compliance, as some participants indicated that they are effective at gaining compliance to renew coverages, but would see items lapse throughout the year.
- Staff development was an area where the business managers indicated a level of demand, stating that they saw the need for and value provided by these services.
- Regulatory compliance (HIPPA, FERPA, and PCI) was viewed as an area where the business managers saw the opportunity to free up existing resources who are already focused on these items if the ISDs were to provide these services.
- Vendor risk assessment and oversight is an item that the business managers felt presented an opportunity for improvement, specifically as it relates to assessing the risks presented by vendor partners. Most business managers felt that they could currently manage vendor contracts effectively.

- Cybersecurity policy development was seen as an area of need by the business managers, as they felt that cybersecurity specific policies were somewhat lacking in their districts.

Business manager scope feedback: SOC

Consistent with the superintendents, business manager participants were not able to comment on the level of need for many of the technical items included in the potential scope for SOC services. They generally highlighted the need for robust phishing assessments and mobile device management (particularly for itinerant and operations staff), but deferred to their IT colleagues in most other areas in this discussion.

Other feedback from business managers

Business managers echoed the desire for a-la-carte pricing for these services to allow for flexibility. They also provided feedback regarding the potential use of remote resources to provide these services, with the general consensus being that the expertise and responsiveness to resources was a greater priority than having someone physically on-site. Business managers did highlight the need for these resources to have expertise in the K-12 education industry as well as cybersecurity.

The following is a snapshot of the level of demand indicated by participating business managers for each potential scope component discussed.

- High (↑): Represents a high level of demand/services in this area are greatly needed
- Medium (▬): Represents a moderate level of demand/services in this area are somewhat needed
- Low (↓): Represents a low level of demand/services in this area are not needed

DEMAND FROM BUSINESS MANAGERS			
CISO SERVICES		SOC SERVICES	
• Strategy, planning, and budgeting	↑	• Penetration testing and vulnerability scanning	Cannot rate
• Risk assessment	↑	• Identity and access management	Cannot rate
• DRP/BIA development and testing	↑	• Phishing assessments	↑
• IRP development and testing	↑	• Threat intelligence and identification	Cannot rate
• Cybersecurity insurance compliance	↓	• Endpoint detection and response	Cannot rate
• Staff development	↑	• Log aggregation	Cannot rate
• Regulatory compliance	↑		
• Vendor risk assessment and management	↑	• Mobile device management	↑
• Policy development	↑		

TECHNOLOGY DIRECTOR FOCUS GROUPS

There were 21 total attendees across the three service regions participating in the technology director focus groups.

ATTENDEES		
KENT ISD	MUSKEGON AREA ISD	OTTAWA AREA ISD
9 total districts	6 total districts	12 total districts

Technology director scope feedback: CISO

- Strategy, planning, and budgeting is an area of need from the technology directors' perspective, particularly given their current limited capacity to perform these activities. Participants also expressed a desire for expertise on the current threat landscape to inform their own planning and budgeting activities.
- Risk assessments are an item where a significant need was expressed, particularly as it relates to comprehensive assessments that would encompass all aspects of cybersecurity at their districts. This would take the place of the limited risk assessments that the participants indicated that they are currently able to conduct.
- Disaster recovery plan/continuity of operations plan development and testing is confirmed by technology directors to be an 'in progress' item with most districts, with some level of plan development completed but limited testing done. Most participants indicated that they have been able to develop a limited plan based on templates provided by their ISDs, but have not been able to complete or test those plans.
- Incident response plan development and testing was noted as being in the same state as DRP/BIA, with limited 'draft' plans having been developed but not completed or tested. DRP and IRP are areas in which the technology directors indicated that significant demand exists for supplemental services.
- Cybersecurity insurance requirements discussions revealed that the technology directors generally agreed with the superintendents and business managers in that there currently is not a high level of need for assistance. They did agree that there may be future demand in this area as those requirements continue to evolve and expand.
- Staff development discussions with technology directors tended to center around IT staff development rather than end users. Participants indicated that assistance with creating professional development plans related to cybersecurity for their staff would be an item of significant value.
- Regulatory compliance (HIPPA, FERPA, and PCI) was viewed as an area where, similarly to the business managers, the technology directors saw the opportunity to free up existing resources who are already focused on these items if the ISDs were to provide these services.
- Vendor risk assessment and oversight is another item where the technology directors tended to agree with the business managers in that the opportunity for improvement was specifically

related to assessing the risks presented by vendor partners. Most technology directors felt that they could currently manage vendor contracts effectively.

- Cybersecurity policy development was seen as an area where technology directors felt that significant assistance was not needed. Participants did indicate that assistance operationalizing those policies with documented procedures was an area of need.

Technology director scope feedback: SOC

- Penetration testing and vulnerability scanning was seen as an area where technology directors felt that significant assistance was needed, particularly in regard to penetration testing.
- Identity and access management was cited as an area of need, however, questions arose regarding the complexity of implementing this solution across multiple districts with disparate Active Directory and/or Google authentication schemes.
- Phishing assessments were seen as an area of low need given that many districts have already begun to implement these assessments independently.
- Threat intelligence and identification was viewed as an area of high need by technology directors. The ability to provide an enterprise security information and event management (SIEM) solution across the region would be highly beneficial.
- Endpoint detection and response was viewed as another component of a SIEM solution and would be highly in demand.
- Log aggregation is the final scoping component that would be provided by a SIEM solution and would again be highly in demand.
- Mobile device management was seen as a lesser need given the proliferation of Chromebooks in most environments and the existing management tools for those devices.

Other feedback from technology directors

Technology directors echoed some of the same concerns as the business managers in that any CISO resources would need a high level of K-12 expertise in addition to the requisite cybersecurity skillsets. They also raised questions related to overall governance and integration of CISO resources into their teams, with the feedback being that they would want this to be a consultative relationship rather than bringing on a true executive leadership position into the organizations. Finally, they expressed concerns that shared CISO resources across a consortium might lead to a lack of understanding of individual district needs and result in ‘cookie cutter’ solutions.

The following is a snapshot of the level of demand indicated by participating technology directors for each potential scope component discussed.

- High (↑): Represents a high level of demand/services in this area are greatly needed
- Medium (▬): Represents a moderate level of demand/services in this area are somewhat needed
- Low (↓): Represents a low level of demand/services in this area are not needed

DEMAND FROM TECHNOLOGY DIRECTORS			
CISO SERVICES		SOC SERVICES	
Strategy, planning, and budgeting	↑	Penetration testing and vulnerability scanning	↑
Risk assessment	↑	Identity and access management	—
DRP/COOP development and testing	↑	Phishing assessments	↓
IRP development and testing	↑	Threat intelligence and identification	↑
Cybersecurity insurance compliance	↓	Endpoint detection and response	↑
Staff development	↑	Log aggregation	↑
Regulatory compliance	↑		
Vendor risk assessment and management	↑	Mobile device management	—
Policy development	↑		

Preliminary scope of services

Based on the results of the survey and focus group activities detailed above, the following preliminary scope of services was developed. The tables below provide a high-level description of each scope component, as well as the level of risk to districts without these services and the general level of cost/effort to implement them independently. This scope was reviewed with the project Steering Committee for approval prior to proceeding with additional activities in the study.

- **Chief information security officer** services provide functions generally performed by an individual responsible for the organization's information security function (e.g., CISO, IT, compliance, etc.). Included within this service grouping are cyber strategy, incident readiness and response, and training and awareness.
 - **Cyber strategy** includes CISO related services that assist in overall cybersecurity strategy and governance related processes. These services are intended to help an organization effectively plan and budget for cybersecurity related countermeasures with a risk-based approach.
 - **Incident readiness and response** includes CISO related services that assist the organization in preparing for and responding to cybersecurity incidents. These services will help ensure the organization can effectively recover from cybersecurity incidents and related business interruptions effectively.
 - **Training and awareness** includes CISO related services that assist the organization in facilitating user and IT staff training initiatives. These services will help the organization ensure their workforce members are properly trained and tested on their cybersecurity responsibilities.

The following tables show the preliminary scope in each category for CISO and SOC. Risk and cost/effort are categorized as follows:

- High (↑): High risk to operations/vulnerability to an incident. Significant effort and cost associated with districts implementing this scope independently.
- Medium (—): Moderate risk to operations/vulnerability to an incident. Moderate effort and cost associated with districts implementing this scope independently.
- Low (↓): Low risk to operations/vulnerability to an incident. Low effort and cost associated with districts implementing this scope independently.

CISO SERVICES: CYBER STRATEGY			
SCOPE	DESCRIPTION	RISK	COST/ EFFORT
Planning and budgeting	Services to support management in their ongoing cyber related budgeting processes, from planning to tracking of actual spend.	↑	↓
Risk assessment	Services to support management in the performance of formal risk assessment processes utilizing generally accepted frameworks (e.g., NIST CSF, CIS, etc.). Also, include risk assessment of third-party vendor contracts.	↑	↑
Policy development	Services to support management in the development of applicable policies, standards, and procedures to support the implementation of a cybersecurity program.	—	—
Regulatory compliance	Services to support management in regulatory compliance (e.g., FERPA, HIPAA, PCI, etc.) related to readiness and reporting obligations.	↑	↑

CISO SERVICES: INCIDENT READINESS AND RESPONSE			
SCOPE	DESCRIPTION	RISK	COST/ EFFORT
IRP development and testing	Services to support management in the development, updates, and ongoing testing of incident response plans.	↑	↑
Continuity of operations plan development and testing	Services to support management in the development, updates, and ongoing testing of business continuity plans.	↑	↑
DRP development and testing	Services to support management in the development, updates, and ongoing testing of disaster recovery plans.	↑	↑

CISO SERVICES: TRAINING AND AWARENESS			
SCOPE	DESCRIPTION	RISK	COST/ EFFORT
Staff skills training (IT)	Services to support management in the evaluation and skills-based training for IT resources, with a focus on cybersecurity related responsibilities.	↑	↑
Security awareness training (end users)	Services to support management in facilitating regular user security awareness training through a formal program and multiple delivery mechanisms (training systems, newsletters, etc.).	↑	—
Phishing	Services to support management in performing periodic phishing assessments to test user's ability to spot and report phishing attempts.	↑	↓

- **Security operations center** services provide functions generally performed by a dedicated group within the organization whose sole responsibility is to identify and respond to security related matters. Included within this service grouping are user and device management, logging and monitoring, and assessment and threat intelligence.
 - **User and device management** includes SOC related services that assist the organization in managing user accounts and devices. These services will help the organization ensure users and devices are inventoried and security controls are applied based on the risk rating of the account or device.
 - **Logging and monitoring** includes SOC related services that assist the organization in the setup, upkeep, and monitoring of critical security log data. These services will help the organization ensure that proper logs are collected to support forensic investigation and that alerting mechanisms are tuned with a risk-based approach.
 - **Assessment and threat intelligence** includes SOC related services that assist the organization in assessing the effectiveness of implemented countermeasures and identifying threats and vulnerabilities to be remediated. These services will help the organization identify risks that exceed their tolerable risk threshold and remediate them before they can be exploited by malicious actors.

SOC SERVICES: USER AND DEVICE MANAGEMENT			
SCOPE	DESCRIPTION	RISK	COST/ EFFORT
Identity and access management	Services to support management in user management functions such as onboarding, terminations, access review, etc.	↑	—
Mobile device management	Services to support management in device enrollment, security control implementation, and support.	↑	—
SOC SERVICES: LOGGING AND MONITORING			
SCOPE	DESCRIPTION	RISK	COST/ EFFORT
Managed detection and response	Services to support management in the implementation, maintenance, and monitoring of the MDR solution on endpoints.	↑	↑
Log aggregation/SEIM	Services to support management in the implementation, maintenance, and monitoring of logging configurations and alerting mechanisms.	—	↑

SOC SERVICES: ASSESSMENT AND THREAT INTELLIGENCE			
SCOPE	DESCRIPTION	RISK	COST/ EFFORT
Threat intelligence	Services to support management in proactive threat detection and monitoring for the organization.	—	—
Penetration testing	Services to support management in the identification of exploitable vulnerabilities from the perspective of an actual internal or external malicious actor.	↑	↑
Vulnerability assessments	Services to support management in performing regular vulnerability scans to identify and remediate vulnerabilities based on risk.	↑	—

ISD capability assessments



ISD capability assessments

Note that our full capability assessments for each ISD have been intentionally omitted from the final version of this study. The purpose for this omission is to protect any potential cybersecurity vulnerabilities in a publicly available document. We will address this topic in terms of generalities that support the recommendations of the study. Also note that we have met with the ISDs to review the detailed observations and recommendations that are not provided in this final report.

The three ISDs vary widely in the size of both the supported districts and their associated IT departments. There are varying levels of participation for ISD districts in their service offerings. This spans from 100% participation by Muskegon ISD districts to 50% participation by Ottawa ISD districts. Additionally, service offerings can vary district to district within each ISD. This can include anything from full IT support services (completely outsourced to the ISD) down to as needed IT support.

From a cybersecurity expertise perspective, all ISDs showed competency and understanding of basic cybersecurity principles. IT related services (including cybersecurity related functions) are generally outlined within a service catalog (or equivalent) document created by each ISD. Billing arrangements vary by ISD and constitute anything from direct billing to allocation to specific school funds.

Current service catalogs and agreements do not always explicitly call out cybersecurity services and, in some cases, cybersecurity related services are provided free of charge due to a lack of specificity within the overall agreement or a lack of time-based billing for problem resolution.

The result of our assessments leads to the conclusion that while each ISD possesses distinct capabilities and maturities in their cybersecurity posture, we would rate all three organizations in the moderately capable to highly capable category for the in-scope areas for CISO and SOC services in this study. The challenges that we were able to observe are related to capacity rather than capability. None of the three ISDs are positioned to offer new cybersecurity services to their constituents without augmenting their current staffing levels. Opportunity also exists to improve internal governance and processes as it relates to the delivery of services, as noted above with our observations related to service catalogs.

Feasibility study



Feasibility study

To assess the feasibility of the ISDs providing CISO and SOC services to their constituent districts and charter schools, we conducted market research to determine budgetary costs for a variety of factors that would impact the service delivery model. We also developed and documented certain assumptions regarding district profiles and the levels of effort that would be required to support them.

Local district profile assumptions

Using publicly available data from the State of Michigan's Center for Educational Performance and Information (CEPI), we developed profile assumptions for what constitutes a small, medium, and large local district in the service region for this study based on total staff full-time employees (FTE). Note that the CEPI data set used was from the 2022-23 school year. Those assumptions were as follows:

- Small districts have under 350 total staff FTE
- Medium districts have 351 to 750 total staff FTE
- Large districts have over 751 total staff FTE

We then developed assumptions regarding the number of IT endpoints at each district based on student counts (headcount), total staff counts (FTE), and teacher counts (FTE). This was again based on CEPI data from the 2022-23 school year. Those assumptions, resulting in the endpoint counts in the table below, were as follows:

- Every student has a single device resulting in a 1:1 ratio of students to endpoints.
- Every staff has a single device resulting in a 1:1 ratio of staff to endpoints.
- One wireless access point is deployed per every 15 students.
- One network connected physical security device (IP video camera, door access control) is deployed per every 45 students.
- One computer lab device is deployed per every 100 students.
- One network connected classroom technology device is deployed per every 14 students.

LOCAL DISTRICT SIZING ASSUMPTIONS					
PROFILE	ASSUMPTIONS	KENT ISD	MUSKEGON ISD	OTTAWA ISD	TOTALS
Small districts	Under 350 staff and 3,500 endpoints	7	8	4	19
Medium districts	351 – 750 staff and 3,501 to 7,500 endpoints	9	4	3	16
Large districts	Over 751 staff and 7,501 endpoints	4	0	4	8
TOTALS		20	12	11	43

CISO effort assumptions by district profile

Using the preliminary scope of services defined earlier in this study, we developed assumptions regarding the level of effort required for a CISO resource to support a single small, medium, and large district on an annual basis.

CISO ANNUAL EFFORT ASSUMPTIONS				
CATEGORY	SCOPE COMPONENT	SMALL DISTRICT	MEDIUM DISTRICT	LARGE DISTRICT
Cyber strategy	Planning and budgeting	40	40	40
	Risk assessment	40	50	60
	Policy development	40	40	40
	Regulatory compliance	60	80	100
Incident readiness and response	IRP development and testing	40	50	60
	COOP development and testing	40	50	60
	DRP development and testing	40	50	60
Training and awareness	Staff skills training (IT)	20	40	60
	Security awareness training (end users)	30	50	70
	Phishing assessments	20	20	20
HOURS PER DISTRICT		370	470	570
FTE PER DISTRICT		0.21	0.26	0.32
MAX DISTRICTS PER FTE		5	4	3
TOTAL HOURS		1850	1880	1710
MODEL FTE COUNT		1.03	1.04	.95

Included in this model is the assumption that a single FTE of CISO human resource would be able to contribute 1,800 effort hours annually (2,080 full-time hours less 160 hours of time off and 120 'administrative' hours that would not be spent serving constituent districts). It also assumes that enough margin for error exists to allow for the small and medium district models to slightly exceed 1.0 FTE capacity in the number of districts a single resource can support.

CISO staffing cost assumptions

In order to determine staffing costs the ISDs will incur for CISO resources, we compared the costs to directly hire resources versus contracting with a third-party vendor for CISO services. This included research on compensation costs in key west Michigan markets as well as identification of budgetary costs to contract for services obtained via an RFI process.

WAGE AND BENEFITS COSTS

Utilizing data from the Economic Research Institute’s Salary Assessor Survey (data as of Oct. 1, 2024) we identified compensation costs for key cybersecurity positions. The following assumptions were used when pulling the data:

- The following job markets were included, however, an analysis of the data showed less than a 2% difference in costs between these markets so an average is presented below:
 - Grand Rapids, Mich. (49525)
 - Holland, Mich. (49424)
 - Muskegon, Mich. (49442)
- Industry: Public Elementary and Secondary Education (K-12) | NAICS code 923110
- Job titles and profiles for both chief information security officer and cybersecurity director were utilized, with the following minimum qualifications:
 - Seven to 10 years of experience
 - Master’s degree
 - Certified Information Systems Security Professional (CISSP) certification
- Base compensation figures include salaries and any bonus reported.
- A factor of 1.4x was applied to compensation amounts to calculate fully loaded FTE costs including benefits.

CISO COMPENSATION: ANNUAL COSTS			
	LOW RANGE (10TH PERCENTILE)	MEDIAN	HIGH RANGE (90TH PERCENTILE)
CISO Base compensation	\$175,652	\$243,164	\$332,977
CISO Benefits (1.4x)	\$70,261	\$97,266	\$133,191
CISO total compensation	\$245,912	\$340,430	\$466,167
Director Base compensation	\$121,020	\$159,749	\$210,424
Director Benefits (1.4x)	\$48,408	\$63,899	\$84,170
Director total compensation	\$169,427	\$223,648	\$294,594

CONTRACTED CISO SERVICES COSTS

We developed and released an RFI to the managed services provider vendor community to understand the costs involved if the ISDs were to contract for CISO services. Vendors were asked to provide budgetary costs for a single small, medium, and large district each (based on the assumptions defined previously in this study). They were also provided the preliminary scope of services for CISO to properly scope their responses. Four responses were received to the RFI, which are summarized below. (Note that one could reasonably expect these costs to decrease in a true competitive bidding environment.)

CISO CONTRACTED COST SUMMARY: ANNUAL COSTS					
	VENDOR 1	VENDOR 2	VENDOR 3	VENDOR 4	AVERAGE
Small district	\$51,900	\$62,000	\$74,800	\$94,500	\$70,800
Medium district	\$75,950	\$80,500	\$112,800	\$189,000	\$150,606
Large district	\$102,100	\$105,500	\$153,400	\$283,500	\$161,125

COST COMPARISON

An analysis of the costs to directly hire versus contract for CISO resources is presented below. Note the following assumptions in this analysis:

- CISO compensation costs
 - Cybersecurity director costs are used rather than CISO. This is intended to reflect that a resource with those qualifications can be reasonably expected to provide the services defined in our CISO scope. It also presents a more cost-effective service delivery model allowing the ISDs to serve a greater number of local districts and charter schools.
 - \$5,000 has been allocated annually for maintenance and upkeep of CISO certifications.
 - The median of the average compensation costs across the three markets is used.
 - An additional CISO resource is hired at each max districts per FTE threshold defined in the effort assumptions table above.
- Contracted services costs
 - The average of all costs received is used in the analysis to reflect variations in scope proposed by the vendors.
 - Vendor costs scale linearly as each additional district is added to the model and do not assume unit price decreases as additional districts are brought on. It is reasonable to expect that increased buying power could be leveraged to reduce vendor costs in this scenario.

- Note that green costs represent lower costs in the following tables while red costs represent higher costs.

SMALL DISTRICT COST COMPARISON			
	HIRED RESOURCES		CONTRACTED RESOURCES
Quantity of districts	CISO resources required	Cost to hire	Cost to contract
1	1	\$228,648	\$70,800
2	1	\$228,648	\$141,600
3	1	\$228,648	\$212,400
4	1	\$228,648	\$283,200
5	1	\$228,648	\$354,000
6	2	\$457,296	\$424,800
7	2	\$457,296	\$495,600
8	2	\$457,296	\$566,400
9	2	\$457,296	\$637,200
10	2	\$457,296	\$708,000
11	3	\$685,944	\$778,800
12	3	\$685,944	\$849,600

MEDIUM DISTRICT COST COMPARISON			
	HIRED RESOURCES		CONTRACTED RESOURCES
Quantity of districts	CISO resources required	Cost to hire	Cost to contract
1	1	\$228,648	\$150,606
2	1	\$228,648	\$301,213
3	1	\$228,648	\$451,819
4	1	\$228,648	\$602,425
5	2	\$457,296	\$753,031
6	2	\$457,296	\$903,638
7	2	\$457,296	\$1,054,244
8	2	\$457,296	\$1,204,850
9	3	\$685,944	\$1,355,456
10	3	\$685,944	\$1,506,063
11	3	\$685,944	\$1,656,669
12	3	\$685,944	\$1,807,275

LARGE DISTRICT COST COMPARISON			
	HIRED RESOURCES		CONTRACTED RESOURCES
Quantity of districts	CISO resources required	Cost to hire	Cost to contract
1	1	\$228,648	\$161,125
2	1	\$228,648	\$322,250
3	1	\$228,648	\$483,375
4	2	\$457,296	\$644,500
5	2	\$457,296	\$805,625
6	2	\$457,296	\$966,750
7	3	\$685,944	\$1,127,875
8	3	\$685,944	\$1,289,000
9	3	\$685,944	\$1,450,125
10	4	\$914,592	\$1,611,250
11	4	\$914,592	\$1,772,375
12	4	\$914,592	\$1,933,500

Costs for services and local district ROI - CISO

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

In this model, local districts would pay their share of one FTE based on their profile, or \$48,016, \$59,448, and \$73,167 for small, medium, and large districts, respectively.

SOC cost assumptions

We identified estimated costs for an ISD to implement and staff their own SOC, to be used in comparison to costs to contract SOC as a service from a managed services provider. Note that these costs do not include any physical construction or ongoing upkeep costs for the SOC, but rather are focused on the staff and technologies that would be required to implement the service.

SOC IMPLEMENTATION COSTS

Our assumptions regarding the staffing and technology requirements for the implementation of a SOC are as follows:

- Staffing to consist of a cybersecurity manager and three specialists. Compensation data is from the ERI survey, using the same assumptions as above with the following exceptions:
 - Three to five years of experience required
 - Master's degree and CISSP certification optional for the cybersecurity manager
- \$5,000 has been allocated annually for maintenance and upkeep of staff certifications.
- Technologies included are:
 - SEIM including set-up and ongoing costs for increments of 200GB per day of log data
 - Small districts assumed to produce 33.22GB of data daily
 - Medium districts assumed to produce 36GB of data daily
 - Large district assumed to produce 40.4GB of data daily
 - EDR solution including ongoing costs (no set-up is included as it is assumed that existing licensing will be leveraged) for endpoint increments as follows (note that these counts do now include IOT or student devices, assumed to be Chromebooks for the purposes of this study):
 - Small district: 300 endpoints protected
 - Medium district: 500 endpoints protected
 - Large district: 1,000 endpoints protected
 - Vulnerability scanning solution with one license per district
 - End-user technology allocation is provided for SOC staff

SOC STAFF COMPENSATION: ANNUAL COSTS			
	LOW RANGE (10TH PERCENTILE)	MEDIAN	HIGH RANGE (90TH PERCENTILE)
Manager Base compensation	\$101,950	\$119,214	\$141,800
Manager Benefits (1.4x)	\$40,780	\$47,686	\$56,720
Manager total compensation	\$142,730	\$166,900	\$198,520
Specialist Base compensation	\$71,653	\$83,276	\$98,899
Specialist Benefits (1.4x)	\$28,661	\$33,310	\$39,559
Specialist total compensation	\$100,315	\$116,586	\$138,458
Three specialists total compensation	\$300,945	\$349,758	\$415,374

We would again use the median of the average compensation costs in determining overall labor costs for a SOC. Based on the data above, those costs are assumed to be **\$536,658** (including costs to maintain certifications of \$20,000).

SOC TECHNOLOGY: YEAR ONE COSTS			
COMPONENT	SET-UP COST	ANNUAL ONGOING COST	TOTAL YEAR ONE COST
SEIM solution	TBD based on scale	Small: \$36,842 Medium: \$43,750 Large: \$87,500	Small: \$36,842 Medium: \$43,750 Large: \$87,500
MDR solution (\$40 per endpoint annually)	Existing	Small: \$12,000 Medium: \$20,000 Large: \$40,000	Small: \$12,000 Medium: \$20,000 Large: \$40,000
Vulnerability scanning solution	N/A	\$4,000 per district	\$4,000 per district
Staff end-user technology*	\$5,000	N/A	\$5,000

MDR solution costs are based on licensing costs obtained via the MI-SECURE initiative. Based on the data above, we anticipate incremental added costs of **\$52,842**, **\$67,750**, and **\$131,500** for each small, medium, and large district onboarded to the service, respectively. Staff end-user costs are assumed to be carried by the ISDs as general overhead costs.

CONTRACTED SOC COSTS

We utilized the RFI process referenced early in this study to obtain budgetary costs for SOC services from managed services providers. Again, vendors were asked to base their responses on the district profile assumptions and preliminary scope of services developed through the study. A summary of those responses is below.

SOC CONTRACTED COST SUMMARY: ANNUAL COSTS				
	VENDOR 1	VENDOR 2	VENDOR 3	VENDOR 4
Small district	\$71,892 +	\$124,000 to \$476,000	\$1,092,000	No response
Medium district	\$124,660 +	\$476,000 to \$928,000	\$1,092,000 to \$2,340,000	No response
Large district	\$172,500 +	\$928,000 +	\$2,340,000 +	No response

SOC COST ANALYSIS

When analyzing the costs to establish a SOC at the ISDs we are unable to provide a comparison against those costs to contract for services from a managed services provider. RFI responses received include all endpoints from the original assumptions for small, medium, and large districts. Upon analyzing costs, it became apparent that IOT devices and student Chromebooks needed to be excluded from EDR cost calculations, preventing an ‘apples-to-apples’ analysis from being realistically possible.

The figures presented below represent estimates of the costs required to implement SOC services at each of the three ISDs in this study. These costs assume full participation from local districts in each service region, but do not include participation from charter schools.

SOC IMPLEMENTATION COSTS: FULL DISTRICT PARTICIPATION			
	KENT ISD	MUSKEGON ISD	OTTAWA ISD
Fixed costs			
Fixed labor cost	\$536,658	\$536,658	\$536,658
Fixed technology cost	\$55,000	\$55,000	\$55,000
Indirect costs (2.5%)	\$14,791	\$14,791	\$14,791
Contingency (5%)	\$29,583	\$29,583	\$29,583
Total fixed costs	\$636,032	\$636,032	\$636,032
Variable costs			
Small districts	7 @ \$52,842 \$369,894	8 @ \$52,842 \$422,736	4 @ \$52,842 \$211,368
Medium districts	9 @ \$67,750 \$609,750	4 @ \$67,750 \$271,000	3 @ \$67,750 \$203,250
Large districts	4 @ \$131,500 \$526,000	n/a	4 @ \$131,500 \$526,000
Total variable costs	\$1,505,645	\$693,737	\$940,618
GRAND TOTAL	\$2,141,677	\$1,329,769	\$1,576,651

Note that this model assumes the implementation of individual SOC's at each ISD, which represents inefficiencies regarding fixed costs. A single SOC serving the entire consortium would provide savings on fixed labor costs, indirect costs, and contingency funds.

Pricing model

In developing a pricing model for CISO and SOC services, we have made the following assumptions:

- The same local district sizing assumptions are used as those in the cost models in this study. Note that these profiles will likely need to be refined as the ISDs get a better understanding of which local districts and charter schools might participate in the program.
- For CISO services, local district costs will be their equal share of directly hired resources by the ISDs.
- SOC cost models are shown individually for each ISD, as well as in a consortium model with all three ISDs jointly operating a single SOC. They are also shown assuming full participation from

local districts as well as 50% participation. In each model, participating districts equally share fixed labor and technology costs.

- ROI calculations for SOC services do not assume a full SOC implementation at the same staffing levels as the ISDs. They do assume:
 - A single cybersecurity manager resource would need to be hired at \$166,900. Note that this resource could also potentially serve in a CISO role for the local district in this model.
 - Fixed technology costs of \$155,250 for SEIM, vulnerability scanning, and staff technology, plus \$15,000, \$25,000, or \$54,000 for EDR.
 - 5% program contingency.

Costs for services and local district ROI - SOC

SOC SERVICE COSTS: FULL DISTRICT PARTICIPATION/INDIVIDUAL SOCS							
		KENT ISD (20 DISTRICTS)		MUSKEGON ISD (12 DISTRICTS)		OTTAWA ISD (11 DISTRICTS)	
	Variable tech costs	Share of total fixed costs	Total cost per district	Share of total fixed costs	Total cost per district	Share of total fixed costs	Total cost per district
Small districts	\$52,842	\$31,802	\$84,644	\$53,003	\$105,845	\$57,821	\$110,663
Medium districts	\$67,750		\$99,552		\$120,753		\$125,571
Large districts	\$131,500		\$163,302		N/A		\$189,321

SOC SERVICE COSTS: FULL DISTRICT PARTICIPATION/JOINT SOC			
		CONSORTIUM (43 DISTRICTS)	
	Variable tech costs	Share of total fixed costs	Total cost per district
Small districts	\$52,842	\$14,791	\$67,634
Medium districts	\$67,750		\$82,541
Large districts	\$131,500		\$146,291

SOC SERVICE COSTS: 50% DISTRICT PARTICIPATION/INDIVIDUAL SOCS							
		KENT ISD (10 DISTRICTS)		MUSKEGON ISD (SIX DISTRICTS)		OTTAWA ISD (SIX DISTRICTS)	
	Variable tech costs	Share of total fixed costs	Total cost per district	Share of total fixed costs	Total cost per district	Share of total fixed costs	Total cost per district
Small districts	\$56,000	\$63,603	\$119,603	\$106,005	\$162,005	\$106,005	\$162,005
Medium districts	\$74,000		\$137,603		\$185,005		\$180,005
Large districts	\$144,000		\$207,603		N/A		\$250,005

SOC SERVICE COSTS: 50% DISTRICT PARTICIPATION/JOINT SOC			
		CONSORTIUM (22 DISTRICTS)	
	Variable Tech Costs	Share of Total Fixed Costs	Total Cost per District
Small districts	\$56,000	\$28,911	\$84,911
Medium districts	\$74,000		\$102,911
Large districts	\$144,000		\$172,911

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

In this model, the ISDs would subsidize the initial build of the SOC, with individual districts paying their incremental share for SEIM, MDR and vulnerability scanning (\$55,842, \$72,750, and \$141,500, respectively).

Cybersecurity liability

The provision of CISO and SOC services by the ISDs presents additional liability exposure from a cybersecurity perspective. We met with two leading insurance carriers for the K-12 industry in Michigan, SET-SEG and Gallagher, to gain a high-level understanding of the risks and potential coverages that may be required if these programs were to be implemented.

Both carriers agreed that, of the services contemplated by this study, SOC services present the greater liability exposure to the ISDs. This is primarily due to CISO services being mainly consultative in nature, while SOC presents the greater possibility that an error by ISD staff could result in a breach or other cyber incident. Both carriers indicated that the need for strong contractual protections would also exist in the services provided. They also indicated that each ISD would need to gauge its own risk tolerance in determining what protections to put in place, citing examples from within Michigan where incidents at local districts which were the result of services provided by their ISDs did not result in litigation or other penalty to the ISDs due to the strong relationship between them.

If the ISDs were to elect for additional liability coverages, one carrier was able to provide a conservative example of a RESA in Michigan that purchased a policy for \$10,000,000 in errors and omissions coverage for approximately \$150,000 annually. Each ISD would need to work with their individual carriers for specific quotes and coverages, however, note that we have not included costs for coverages in our models.

Program recommendations

Recommended scope of services

Based on the feedback received from stakeholders via surveys and focus groups, we were able to confirm that demand exists among the local districts for CISO and SOC related cybersecurity services from the ISDs.

Recommended CISO scope includes:

- **Chief information security officer** services to provide functions generally performed by an individual responsible for the organization's information security function (e.g., CISO, IT, compliance, etc.). Included within this service grouping are cyber strategy, incident readiness and response, and training and awareness.
 - **Cyber strategy** includes CISO related services that assist the organization in overall cybersecurity strategy and governance related processes. These services are intended to help an organization effectively plan and budget for cybersecurity related countermeasures with a risk-based approach.
 - **Incident readiness and response** includes CISO related services that assist the organization in preparing for and responding to cybersecurity incidents. These services will help ensure the organization can effectively recover from cybersecurity incidents and related business interruptions effectively.
 - **Training and awareness** includes CISO related services that assist the organization in facilitating user and IT staff training initiatives. These services will help the organization ensure their workforce members are properly trained and tested on their cybersecurity responsibilities.

Recommended SOC scope includes:

- **Security operations center** services to provide functions generally performed by a dedicated group within the organization whose sole responsibility is to identify and respond to security related matters. Included within this service grouping are user and device management, logging and monitoring, and assessment and threat intelligence.
 - **User and device management** includes SOC related services that assist the organization in managing user accounts and devices. These services will help the organization ensure users and devices are inventoried and security controls are applied based on the risk rating of the account or device.
 - **Logging and monitoring** includes SOC related services that assist the organization in the setup, upkeep, and monitoring of critical security log data. These services will help the organization ensure that proper logs are collected to support forensic investigation and that alerting mechanisms are tuned with a risk-based approach.
 - **Assessment and threat intelligence** includes SOC related services that assist the organization in assessing the effectiveness of implemented countermeasures and identifying threats and vulnerabilities to be remediated. These services will help the

organization identify risks that exceed their tolerable risk threshold and remediate them before they can be exploited by malicious actors.

Recommended service delivery model

Based on the study activities completed to date, we have developed the following recommendations related to a potential service delivery model:

1. **Further investigate a consortium-based implementation for SOC services:** Given the cost models developed through this study, individual SOC implementations do not appear to be cost effective. More detailed plans for the implementation and management of a joint, consortium-based SOC should be developed.

In the event that a single ISD in the Consortium obtains funding to implement their own SOC, the costs outlined in this study for an individual SOC should apply. Such a program could then serve as a 'pilot' that could eventually be scaled for implementation Consortium-wide (and potentially beyond).

2. **Establish a formal governance structure:** Based on the recommended consortium model, formal agreements between the ISDs and governance structures to operate the programs should be developed.
3. **Clarify existing service catalogs:** Based on feedback from the ISDs during the capability assessments, current catalogs for services provided to LEAs and PSAs are somewhat poorly defined. Effort should be given to clearly defining services currently provided to ensure that no appearance of duplication of scope exists between current services and those proposed in this study.
4. **Revisit demand discussions with local districts and charter schools:** To determine whether to proceed with the implementation of CISO and SOC services, the consortium should revisit demand discussions after reviewing potential costs for services with their stakeholders. This will allow for a better understanding of participation levels and for the refinement of costs to the local districts.
5. **Develop a staffing strategy:** Consider staffing and talent acquisition strategies, including local versus remote resources. Stakeholders interviewed indicated that while local resources are preferred, expertise (cybersecurity and K-12 industry expertise) and level of access to those resources were a greater concern. Develop the appropriate job descriptions, and if based in a consortium model, determine which ISD will hire the resources based on established governance structures.
6. **CISO capacity:** Confirm how much 'excess' CISO capacity can be carried operationally to allow for additional districts to be onboarded to the program without the need to hire additional resources.
7. **Develop operating procedures for CISO and SOC:** Document standard operating procedures for both programs to govern how services will be provided and set performance measures.

-
8. **Investigate further scalability for SOC services:** Given the impact of scale on driving down fixed cost shares to districts, determine whether additional ISDs might wish to join the consortium.
 9. **Further investigate outsourcing options:** The RFI process undertaken in this study did not identify the potential buying power at scale if these services are to be outsourced. If this is a strategy the ISDs wish to investigate, a more formal procurement process is recommended.

Recommended cost model

Using the program costs developed as a part of this study, we are recommending the following cost/pricing models for local district and charter school participants.

1. CISO costs should be allocated evenly to program participants based on the level of effort required to support their district. Under the assumptions made in this study, the structure would be to use the fractional FTE calculation applied against the total compensation cost for the resources deployed.

CISO SERVICES COST			
	FTEs REQUIRED	COST TO HIRE ONE FTE	DISTRICT SHARE OF ONE FTE
Small districts	.21	\$228,648	\$48,016
Medium districts	.26		\$59,448
Large districts	.32		\$73,167

2. SOC costs should be allocated as an even share of fixed costs across all participants, plus each district's variable costs for items such as EDR and vulnerability scanning solutions.

SOC SERVICE COSTS: FULL DISTRICT PARTICIPATION/JOINT SOC			
		CONSORTIUM (43 DISTRICTS)	
	Variable tech costs	Share of total fixed costs	Total cost per district
Small districts	\$55,842	\$14,791	\$70,634
Medium districts	\$72,750		\$87,541
Large districts	\$141,500		\$156,291

3. For both CISO and SOC services, we cannot recommend an a-la-carte pricing model as it presents significant challenges in sizing service offerings and determining necessary capacity.

Appendix A: Glossary of acronyms

The following provides definitions for the various acronyms used in this report.

CEPI – Center for Educational Performance and Information: a Michigan government organization that collects, manages, and reports education data.

CIS – Center for Internet Security: an independent, nonprofit organization who develops cybersecurity controls, benchmarks and best practices.

CISO – Chief Information Security Officer: a senior level executive responsible for an organization's information security.

CISSP – Certified Information Systems Security Professional: a cybersecurity certification that demonstrates a professional's ability to design, implement, and manage an organization's cybersecurity program.

COOP – Continuity of Operations Plan: a detailed document that outlines how an organization will continue to perform their mission essential functions during a wide range of emergencies.

CSF – Cybersecurity Framework: the National Institute for Standards and Technology's set of guidelines and best practices that help organizations manage cybersecurity risks.

DRP – Disaster Recovery Plan: a detailed document that outlines how an organization will respond to an unplanned incident.

FERPA – Family Educational Rights and Privacy Act: a federal law that protects the privacy of students' educational records.

FTE – Full Time Equivalent: a unit of measurement that combines the hours of

part-time and full-time employees into a number of full-time positions.

HIPAA – Health Insurance Portability and Accountability Act: a federal law that protects the privacy and security of health information.

IOT – Internet of Things: a network of physical objects, “smart objects”, that can connect to the internet and exchange data.

IP – Internet Protocol: a digital media transport system and network standard.

IRP – Incident Response Plan: a set of instructions or procedures for detecting, responding to, and limiting the consequences of a cyber attack against an organization's information systems.

ISD – Intermediate School District: a government agency in Michigan that provides administrative and educational services to local school districts and charter schools.

LEA – Local Education Agency: a public school/district that operates in accordance with the Michigan Department of Education's policies, regulations, and statutes.

MDR – Managed Detection and Response: a cybersecurity service that uses technology and human expertise to monitor, detect, and respond to cyberthreats.

NAICS – North American Industry Classification System: a six-digit coding system that classifies businesses into industry sectors.

NIST – National Institute for Standards and Technology: a non-regulatory government

agency that develops and evaluates standards, metrics, and technologies.

PCI – Payment Card Industry: compliance standards that businesses must follow to protect credit cardholder data.

PSA – Public School Academy: a publicly funded charter school that operates in accordance with the Michigan Department of Education's policies, regulations, and statutes.

RFI – Request for Information: a formal process used to gather information from potential suppliers of a product or service.

SIEM – Security Information and Event Management: a set of instructions or procedures for detecting, responding to, and limiting the consequences of a cyber attack against an organization's information systems.

SOC – Security Operations Center: a centralized unit that monitors and manages an organization's information security posture.



**Thank you for the opportunity to serve Kent ISD.
Please contact us with any questions.**



Mark Warner
Relationship Partner
248-223-3799
mark.warner@plantemoran.com