Booz | Allen | Hamilton

Commercial Solutions

INFORMATION SHARING AND ANALYSIS CENTER

A Blueprint for Success

July 2014

Booz Allen Hamilton's Commercial Solutions combines industry knowledge and relevant experience with the right people and technologies to reduce risk, improve safety and increase profitability for your business. Together, we can enable you to thrive today, tomorrow and beyond.

EXECUTIVE SUMMARY

Information Sharing and Analysis Centers (ISAC) are centralized organizations that foster and facilitate the secure sharing of vetted, actionable, and timely information among members.

Existing and newly forming ISACs created in specific critical infrastructure (CI) sectors and industry segments provide private sector owners and operators a way to strengthen their organizations and the resiliency of their industry. Recent attacks have highlighted the need for industry to share threat and vulnerability information, and ISACs help members stay out in front of threats and vulnerabilities industries face.

The National Council of ISACs (NCI) formally designates ISACs, defining an ISAC as "a trusted, sector specific membership organization, which provides operational capabilities for its sector consistent with the National Infrastructure Protection Plan."[1] Nascent organizations may find that becoming an official ISAC is appropriate, while others may forego formal designation to become an information sharing and analysis organization. The principles discussed throughout apply to both kinds of organizations; however, for simplicity, the term ISAC is used going forward.

Most ISACs foster the sharing of all-hazards information, to include physical security, while some focus entirely on sharing cybersecurity information. This information may include network breaches and control system attacks, warnings about system disruptions or failures, and other cyber threat intelligence. Sectors that currently have ISACs find sharing this information essential in identifying and mitigating cybersecurity threats to both control and business systems. Subsequently, ISACs operate in a manner to protect members from anti-trust violations and Freedom of Information Act queries. Additionally, ISACs make recommendations to the member community; however, they are not in a position to mandate specific actions. While individual CI sectors or industry segments may find themselves at different states of maturity with respect to the formation of, or interest in, an ISAC, many follow a similar path to progression and growth.

Experience demonstrates that there are common, foundational building blocks necessary to create successful information sharing and analysis organizations. Whether yours is a new ISAC or an existing one looking to mature, these five key building blocks—Governance, Policy, Technology, Culture, and Economics—ensure the solid foundation required for successful implementation. Critical questions include:

- **Governance**: How will the ISAC be governed? Does it have strong leadership with the right industry and functional cybersecurity skills to oversee day-to-day operations?
- **Policy**: Who is eligible for membership?
- **Technology**: What mechanisms exist to manage identities, authorize and authenticate users, ensure confidentiality, and foster information sharing?
- **Culture**: Has the ISAC created a trusted environment where members feel comfortable sharing information?
- **Economics**: How will the ISAC be funded and measure success? How do we ensure that the necessary initial- and build-value are present to create a sound economic model?

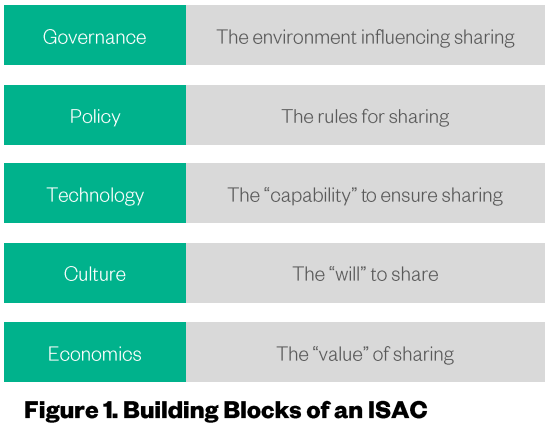


Figure 1. Building Blocks of an ISAC

There are five phases that must occur to create, build, grow, and mature an ISAC. The building blocks are key considerations in each of the five execution phases. This ISAC Blueprint summarizes the five-phase, structured approach to successfully build and mature an ISAC. The principles discussed in each phase are relevant factors for industries to consider when embarking on growing or maturing an ISAC.

[1] National Council of ISACs Charter, September 2012

Figure 2. The Five-Phase Blueprint for ISAC Success

Phase 1: Engage Partners

Three key factors must be considered in Phase 1: The landscape within the specific industry, the key stakeholders involved, and existing information sharing partnerships. Stakeholder engagement focused on these factors helps build the right ISAC start-up team moving forward. Phase 1 consists of two actionable steps:

- **Step 1:** Initiate the ISAC Discussion
- **Step 2:** Determine Essential Partners

Step 1: Initiate the ISAC Discussion

Industries interested in creating an ISAC must collaborate to answer key questions central to ISAC formation. Answering the questions outlined in Figure 3 helps interested stakeholders identify the benefits of creating an ISAC and communicate this need across a large partner base. Answers also set the tone for ISAC formation.

Questions to Initiate the ISAC Conversation	Is there an existing body or mechanism in the sector to facilitate information sharing?
	Is there a strong enough motivation in the sector to create an ISAC for information sharing purposes?
	What value would an ISAC bring to the sector that doesn't currently exist?

Figure 3. Key Questions to Ask when Initiating the ISAC Discussion

Step 2: Determine Essential Partners

All ISACs require a strong level of collaboration among stakeholders to maximize information sharing within a trusted environment. This collaboration must occur between individual companies, visible industry associations, and, as appropriate, supporting government agencies. Cooperation and collaboration across the entities illustrated in Figure 4 is critical to both the stand-up and sustainability of an ISAC. The proper combination and engagement of stakeholders and partners creates interest at the time of ISAC inception and fosters growth as ISAC operations are implemented. Table 1 highlights the roles that partners and stakeholders play during ISAC formation.

Industry Sector Partners	Private sector industry partners are the basis of a successful ISAC. They lead and usually fund ISAC operations. Sector Coordinating Councils (SCCs) can play an important role in coordinating industry sector partners during ISAC formation.
Government Partners	Partnerships with government, for example through the Government Coordinating Council (GCC) and Sector Specific Agency (SSA), can help facilitate information sharing across the industry. They can also provide a mechanism to leverage stakeholders' existing information sharing agreements with government agencies.
ISAC Partners	The National Council of ISACs (NCI) is an important resource for new and established ISACs. NCI facilitates information sharing across sectors. NCI offers a wealth of resources for an emerging ISAC; engaging NCI can help emerging ISACs apply proven processes and models.

Table 1. The ISAC Stakeholder Landscape

Phase 2: Mobilize ISAC Planning Team

Phase 2 of standing-up an ISAC leverages stakeholder discussions and relationships developed in Phase 1 to create and mobilize an ISAC planning team. The ISAC planning team is critical to building the ISAC's foundation and encourages potential members to have a direct hand in its creation. Industry stakeholders must drive the creation of their respective sector's ISAC, as they understand the needs of their specific organizations and the type of ISAC that would benefit the industry. This grassroots effort is essential, as participating companies represent potential members that will join the ISAC; each stakeholder brings to the table unique capabilities and knowledge specific to their segment within the industry. This full-engagement strategy promotes a round table discussion on how to ground the new ISAC and creates a sense of ownership and personal stake in the ISAC's success. Phase 2 consists of two actionable steps.

- **Step 1:** Form a Start-up Leadership Body
- **Step 2:** Develop Working Groups

Figure 4. The Relationship between ISAC Partners and Stakeholders

Step 1: Form a Start-up Leadership Body

Once potential partners are identified and engaged, an ISAC Start-up Leadership Body can be formed. Ultimately, this leadership body will assume the responsibility of providing guidance on the ISAC's overall strategic direction. The leadership body should consist of several high-level, influential stakeholders with extensive experience and expertise who can best represent their industry or sector. The ISAC Start-up Leadership Body is required to make strategic decisions and build stakeholder consensus around all aspects of ISAC formation.

Step 2: Develop Working Groups

Task-focused working groups are a proven way to engage industry. This working group structure allows members to provide specific input for key ISAC Building Blocks in which they have interest or expertise. While each sector or industry segment will have unique desires and concerns, there are seven common areas around which a working group structure can be built. Figure 5 highlights these working groups and their potential responsibilities.

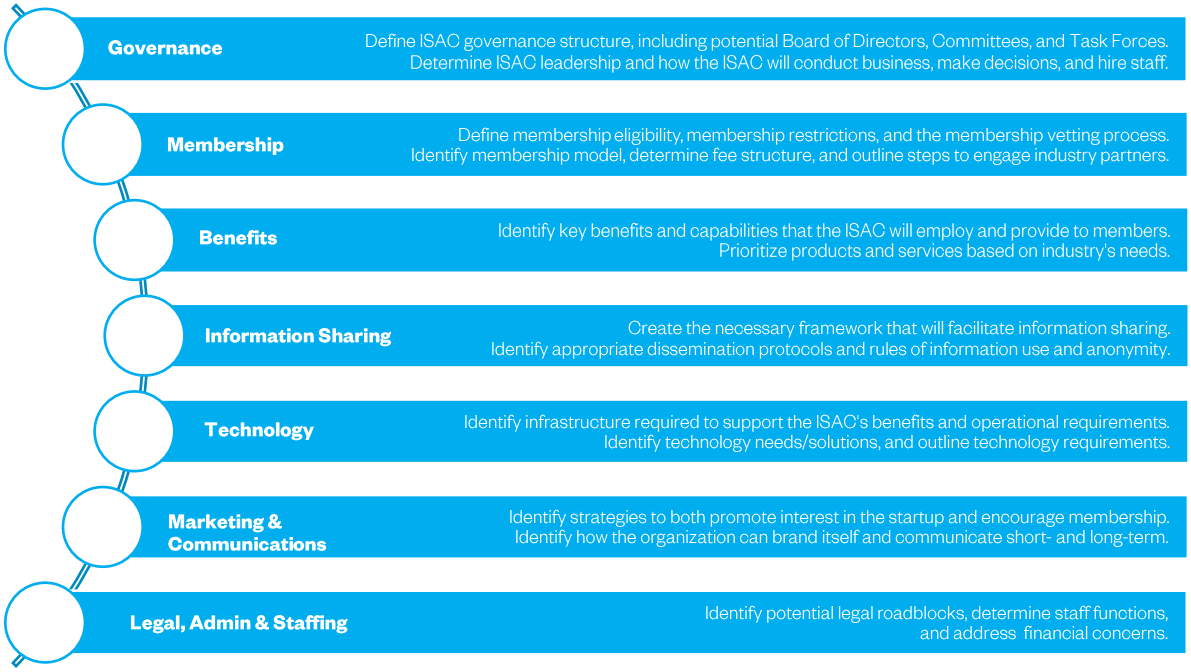


Figure 5. Working Groups and Their Potential Responsibilities

Phase 3: Develop Concept of Operations

The Concept of Operations (ConOps) serves as the ISAC's roadmap to establishment and is the culmination of activity performed in Phase 3. The ConOps encompasses elements that include the five key building blocks of an ISAC—Governance, Policy, Technology, Culture, and Economics. While the exact structure and content of the ConOps will vary for each individual ISAC, a typical ConOps includes key ISAC elements such as: governance structure, membership model, information sharing framework, and other necessary components of the organization. Phase 3 includes two actionable steps:

- **Step 1:** Create a Plan of Action and Milestones (POA&M)
- **Step 2:** Build the Foundation of an ISAC

Step 1: Create a POA&M

Once working groups are established in Phase 2, they must establish a battle rhythm for ConOps creation. The ISAC Start-up Leadership Body must coordinate with the working groups to delegate the ConOps sections specific to their assigned task/area (e.g. membership). While many of the engaged stakeholders will be interested in contributing to every aspect of the ConOps, a well thought out POA&M will focus stakeholder and working group energy and attention on specific questions and process design. Through an iterative process that has designated milestones associated with deadlines and items to be completed, the working groups can work in concert to develop a ConOps in a relatively short period of time.

Step 2: Build the Foundation of an ISAC

In accordance with the POA&M, working group members must first identify the mission, goals, and objectives of the envisioned ISAC. Without an agreed upon scope and identity, it will be difficult for working groups to create cohesive parts that make a whole. As highlighted in Table 2, each working group must answer key questions and contribute important outputs to be included in the ConOps.

	Working Group Output	Key Questions
Governance	Governance Structure *Board of Directors, Committees, Task Forces*	Who can participate in ISAC governance? Who will lead the ISAC?
Membership	Membership Model *Eligibility, Restrictions, Vetting, Fee Structure, External Partners*	Who will decide who can and cannot become a member? Will ISAC membership be restricted by geography? What is the appropriate fee structure?
Benefits	Benefits List *Industry priorities, Intelligence products, Potential tiers*	Will all ISAC benefits be provided to all members? Are certain benefits more of a priority than others?
Information Sharing	Operating Framework *Submission protocols, Dissemination protocols, Rules of use, Operating requirements*	How will anonymity be ensured? How will members be allowed to share information? What type of analysis should the ISAC perform?
Technology	Enabling Tools *Underlying infrastructure, Technology components, Data analytics, Communications support*	What technology requirements are needed? What infrastructure is needed for incident response? What security concerns should be addressed? How can data be protected?
Marketing and Communications	Marketing Strategy *Membership growth, Relationship management, ISAC branding*	How will the ISAC market itself? How can the ISAC brand itself? How will the ISAC continue to market its capabilities?
Staffing, Administration, Legal	Legal Documentation *Certificate of Incorporation, Charter, Operating Rules, Member Agreement*	Where will the ISAC's security operations be located? What staff and analyst skill sets are required? How much will the first year's operations cost? How much revenue can be expected?

Table 2. Working Groups Outputs and Key Questions to Ask

Phase 4: Incorporate and Implement Operations

Following the finalization and leadership approval of the ConOps, and leveraging momentum generated in the first three phases, the ISAC Start-up Leadership Body can move forward with legal formation of the ISAC. Phase 4 consists of actions that accomplish the following: confirm industry interest, market the ISAC, and legally incorporate the ISAC. Once legally established, the ISAC can implement operations, finalize membership, and begin services. A proposed list of events leading up to ISAC incorporation is illustrated in Figure 6.

Accurate timing of Phase 4 activities presents a unique challenge. Unlike Phases 1 through 3, Phase 4 cannot be accomplished in sequential steps. Phase 4 actions must be done in parallel; this complexity stems from the fact that several actions (such as financial/bank paperwork) cannot be completed until the ISAC is recognized as a legal entity.

The ISAC Start-up Leadership Body may make the decision to postpone legal incorporation until they confirm that the organization can launch and sustain operations. The question that must be asked is: Have enough industry stakeholders formally expressed interest in, or committed to, ISAC membership to financially support the organization? The first three events illustrated in Figure 6 are focused on answering this question.

Another complexity of Phase 4 is the action of appropriately setting expectations for inaugural members. Inaugural ISAC members are responsible for driving governance, decision making, and funding activities to launch the organization, and as such, they play an immense role in moving the organization forward. Yet, these members must appreciate that ISAC benefits are not immediately realized. Because of this, members may be hesitant to join the ISAC in its infancy. A successful marketing strategy developed in Phase 3 can set expectations and

address stakeholders' concerns. This Phase 3 action is essential to confirming interest in Phase 4 and moving forward with ISAC incorporation.

Figure 6. Proposed List of Phase 4 Activities

Phase 5: Mature the ISAC

A newly formed ISAC will need to focus on initiating operations and bringing on new members, especially throughout the first several months. This will require a dedicated leadership body and appropriate support staff to ensure that services are acquired and new members can begin information sharing activities. Phase 5 includes three steps:

- **Step 1:** Acquire Operations Infrastructure
- **Step 2:** Build and Manage Member Relationships
- **Step 3:** Mature ISAC Operations

Step 1: Acquire Operations Infrastructure

The newly chosen ISAC leadership will acquire a combination of contracted services and/or individually purchased solutions. This step leverages the requirements defined in Phase 3 by the Legal, Administration, and Staffing Working Group. The foundational elements of an ISAC will consist of underlying technology infrastructure, a secure portal, executive staff, and security analysts. Acquiring cost projections and information organically or via a request for proposal (RFP), leadership can determine what vendors will most successfully deliver these solutions to the ISAC and its members.

An ISAC's expenses are determined by the capabilities provided and the revenue the ISAC receives through membership fees. Some ISACs have built their organization over time, hiring employees and acquiring custom solutions the ISAC directly operates. Alternatively, many ISACs have also hired vendors to provide staffing and existing technical solutions. Because the range of vendors and solutions varies widely, costs associated with different solutions vary accordingly. Table 3 provides a general overview of expenses, revenue, and key considerations required for operations. All numbers are approximated.

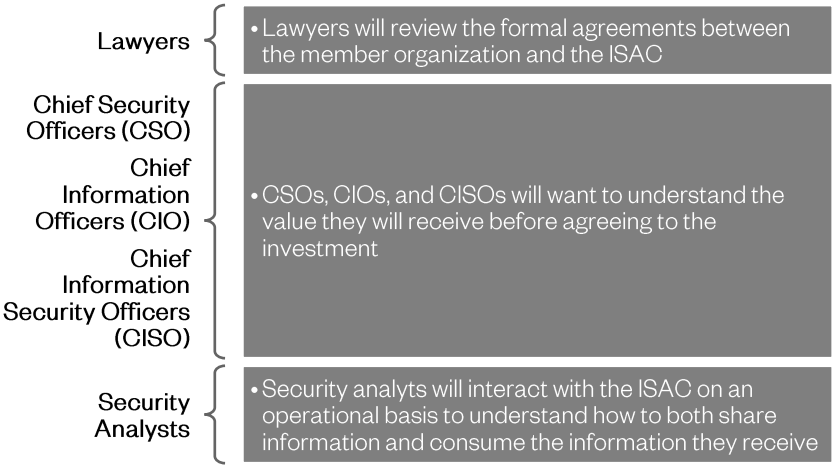
			Annual Revenue and Expense Projections Cost Projections based on level of services chosen		
Revenue/ Expense Stream	**Key Considerations**	**One Time Setup Expense**	**Low**	**Medium**	**High**
Membership Fees	An ISAC with a tiered-membership model can exceed $1 million in annual revenue with 20+ members paying $50,000/year in fees at the highest tier. Strategic Partner programs can generate revenue of ~$10,000-~$20,000/partner. Some ISACs have received seed funding from associations and government agencies.	N/A	+ $1,000,000	+ $2,000,000	+ $3,000,000
Secure Web Portal	The cost of the solutions depends on an ISAC's desire to acquire an existing solution from a vendor or a custom-built solution, both which require some level of maintenance.	~ $100,000* to ~$350,000** *Associated with shared portal **Associated with custom-built solution	$50,000 *Maintenance/ Hosting fees associated with shared server space to host portal*	$75,000 *Maintenance associated with commercial, off-the-shelf portal solution*	$100,000 *Maintenance associated with custom-built solution; portal and server dedicated solely to the ISAC*
Infrastructure and Technology	Technology solutions (including hardware, email, alert notification systems, system security, and licenses) will vary widely in cost. Security infrastructure, such as public key infrastructure (PKI) and authentication tokens, must be purchased specific to the ISAC. Technology costs must take into account the necessity need for large data file storage capacity and intensive processing capabilities. If an ISAC desires physical office space, particularly near other ISACs in the DC area, the cost will increase significantly.	~ $100,000 to ~$500,000	$100,000 *Rental of pre-furbished office space. Purchase of key infrastructure such as PKI tokens and cloud services (limited number of licenses)*	$250,000 *Establishment of physical office space. Purchase of key infrastructure such as PKI tokens and cloud services (increased number of licenses)*	$500,000 *Two physical locations established. Purchase of key infrastructure such as PKI tokens and cloud services (increased number of licenses)*
Project Management and Intelligence Analyst Staff	Program management staff, including an Executive Director (estimated salary ~$200,000) and project managers provide leadership and oversight. Intelligence analysts (Salary ~$125,000) facilitate information sharing between members and partners and correlate the data submitted to the ISAC to identify trends and context.	N/A	$300,000 *Essential Staff Only: Executive Director, only 1 full-time Analyst*	$600,000 *No staffed System Administrator, only 1 full-time Analyst, reduced Support Staff*	$900,000 *Executive Director, Program Manager, System Administrator and ~ 2 full-time Analysts and Supporting Staff*
Threat and Vulnerability Feeds	Several vendors provide data feeds and products that increase the ISAC's ability to provide threat intelligence to members but come at significant cost.	N/A	$75,000 *One vendor contracted to provide monthly threat and vulnerability reports*	$175,000 *One vendor contracted to provide weekly reports, or multiple vendors to provide monthly/ quarterly reports*	$250,000 *Multiple vendors contracted to provide weekly reports, or multiple vendors to provide monthly/ quarterly reports*
Marketing and Outreach	Growing the ISAC and managing member relationships are key components of the ISAC. Developing in-house marketing capabilities will differ in cost from paying for outsourced services.	N/A	$25,000 *Outsourced marketing support limited to material production, reduced personal outreach*	$35,000 *Resources split between outsourced support and in-house capabilities*	$50,000 *Dedicated, in-house marketing support, extensive in-person outreach appearances that require travel*

			Annual Revenue and Expense Projections Cost projections based on level of services chosen		
Revenue/ Expense Stream	**Key Considerations**	**One Time Setup Expense**	**Low**	**Medium**	**High**
Legal Support	Some ISACs will decide to become standalone non-profit organizations and will need to consider incorporation, tax exemption, and banking activities.	~$15,000 to ~$25,000 *Required in ISAC start-up phase. See breakout to right.*	$15,000 *Contracting of incorporation documentation/filing, minimal support associated with other legal matters*	$20,000 *Resources split between outsourced legal and incorporation support and in-house capabilities*	$25,000 *Comprehensive outsourced legal support (financial matters, authoring of Charter/legal documents, insurance & auditing, and incorporation support)*

Expense Projections	**One Time Expense**	**Low Expense Projections**	**Medium Expense Projections**	**High Expense Projections**
ISAC Start-up and Operations Expense Projections, Year 1 only *Includes One-time Expenses, plus Annual Costs*	~$215,000 to ~$875,000	$782,000	$1,685,000*	$2,700,000
Annual ISAC Operations Expense Projections, after Year 1 *Includes only Annual Costs*	n/a	$567,000	$1,140,000	$1,825,000

Year 1 Medium Expense Projection assumed one-time expenses of $545,000

Table 3. Operating Revenue and Expense Considerations



Step 2: Build and Manage Member Relationships

With a legal entity in place, the ISAC can enter into formal agreements with members and accept membership fees. Marketing will continue to remain important throughout this process, but a relationship management strategy is imperative. The new ISAC will interact with important individuals and industry stakeholders. Effective communication with three key stakeholders will ensure that relationships are both created and strengthened. The types of stakeholders, accompanied by their relative interests in and type of interactions with the ISAC, for which the ISAC's relationship management strategy must account are highlighted in Figure 7.

Figure 7. Stakeholders to Consider in the ISAC's Relationship Management Strategy

Step 3: Mature ISAC Operations

Once the ISAC has implemented baseline operations, additional capabilities should phase-in over time to build a more robust organization. To stay relevant, an ISAC must make a concerted effort to continually understand both the cybersecurity landscape and membership needs to ensure capabilities correctly align to the industry's most salient issues and challenges. The use of internal assessments, stakeholder feedback mechanisms, and evaluation against industry cybersecurity maturity models are proven methods of helping ISACs understand where to target capabilities and focus growth. Using the maturity model example, an ISAC could undergo an assessment, benchmark against

other organizations within the industry, hone in on areas for improvement, and establish annual targets for maturity. Furthermore, for the areas of improvement, an ISAC may use some or all of the capabilities listed in Figure 8 to mature operations, stay relevant, and best meet member needs.

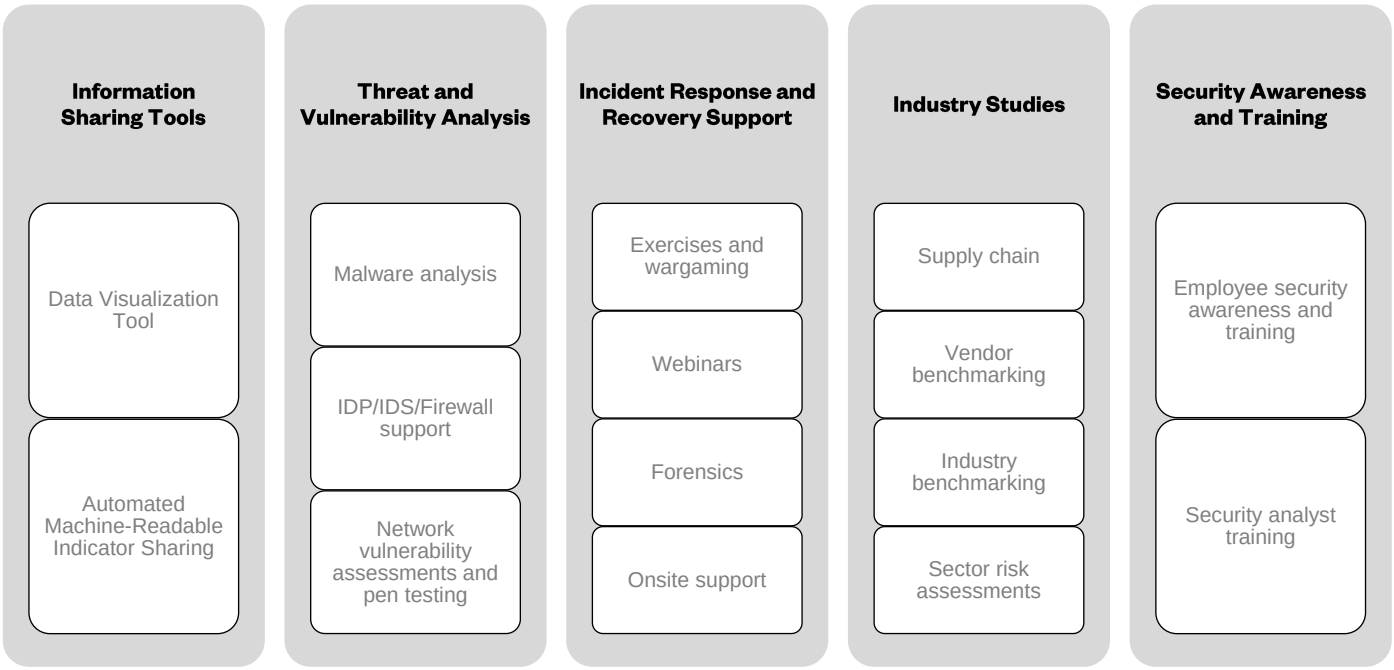


Figure 8. An Array of Capabilities to Help an ISAC Mature

SUMMARY

Each industry faces a unique set of challenges, including but not limited to cybersecurity challenges such as malware, data breaches, and cyber espionage.

Each threat has become more aggressive and sophisticated, and companies are realizing that it's not a question of *if* an attack will happen, but *when*. ISACs are a proven way for companies within an industry to collectively defend against such attacks. Ultimately, an ISAC provides strength in numbers.

There is a proven, five-phased process focused on creating an ISAC. This process defines the foundational building blocks essential for success and shepherds an ISAC from genesis to operational implementation. The ISAC Blueprint is the first step to successfully share information and increase a sector's cybersecurity preparedness and resilience. The next step begins with you.

Figure 9. The Five-Phase Blueprint for ISAC Success

To learn how Booz Allen Hamilton can help your business thrive, contact:

Susan Maly
Lead Associate
+1-703-377-6448
Maly_Susan@bah.com

Susan Maly is a Lead Associate at Booz Allen focused on cybersecurity and Big Data analytics for commercial clients. Ms. Maly blends business, technology, and strategy to develop enterprise cyber security solutions across multiple industries and the public sector. She specializes in strategy, organizational design, information sharing, cyber threat intelligence and analytics, and change management.

Sedar Labarre
Principal
+1-202-346-9201
Labarre_Sedar@bah.com

Sedar Labarre is a Principal and leads Booz Allen's commercial manufacturing, consumer products, and high-tech practice. Mr. Labarre is an industry recognized expert in Cyber Security, Supply Chain Risk Management and Organizational Design and Development and leads a team of diversified functional experts providing cyber security risk management through strategy, policy, analysis, planning, and execution support.

www.boozallen.com

Booz | Allen | Hamilton