IT-ISAC: Beyond Information Sharing

International Cybersecurity Symposium
Tokyo, Japan
November 11, 2019

IT ISAC

What is the IT-ISAC?

What we Are

Information
Sharing &
Analysis
Center

What we Do

Innovate
Share
Analyze
Collaborate

Mission Statement

- Grow a diverse community of companies that leverage information technology and have in common a commitment to cyber-security; to serve as a force multiplier that enables collaboration and sharing of relevant, actionable cyber threat information and effective security policies and practices for the benefit of all.

Value Proposition

The IT-ISAC amortizes the cost of defense by providing a trusted forum for companies to share intelligence, effective practices, and to collaborate to mitigate common threats.

- Serve as a force multiplier by connecting specialized expertise and analysts from across diverse industries
- Receive intelligence from across the national and global critical infrastructure community
- Improve practices to gain, share, consume and leverage tactical and strategic threat intelligence
- Established, trusted and operational—no need to start something new!

The Business Case for Sharing

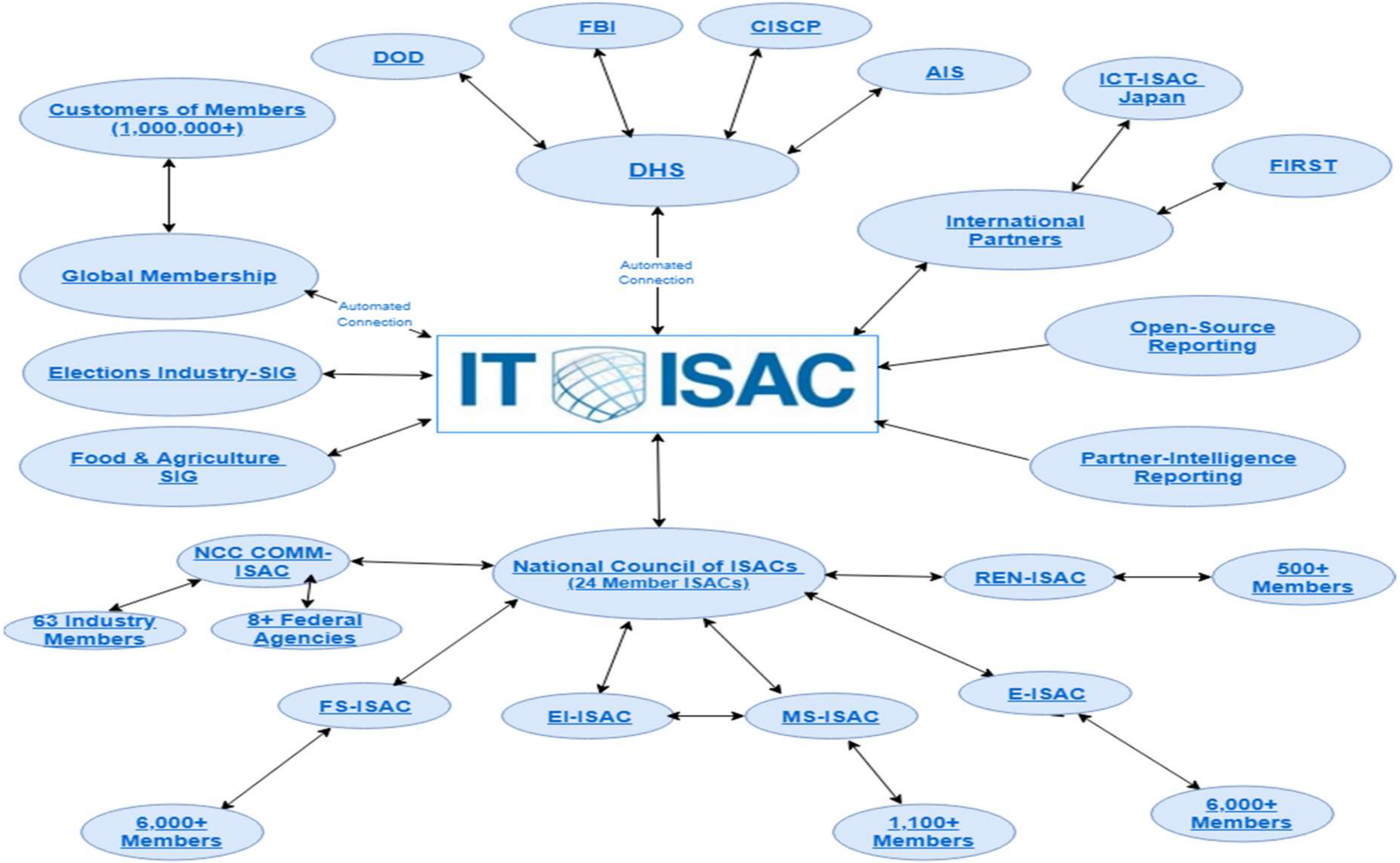
- Sharing is a risk management activity
  - Information sharing is a tool to achieving enhanced situational awareness
  - You get (and provide) early warnings by sharing
- Collaboration amortizes the cost of defense
  - By sharing with others you learn from others
  - Identify actors and threats you may not have been tracking
  - You help your suppliers, partners and competitors secure their enterprises
- Entered an era of increased risk of cyber regulations
  - Demonstrate to stakeholders corporate commitment to protecting its brand, assets, customers, employee and IP
  - Act voluntarily or accept regulatory mandates

IT-ISAC Today

- Global membership from a diverse set of companies that produce, use, and leverage IT products and services for core business operations.
- Supports 3 Critical Infrastructure Sectors—IT, Food and Agriculture, and Elections Industry.
- Focus is on threats to enterprises and core business processes and functions.
- Established, formalized partnerships across critical infrastructure ISACs.

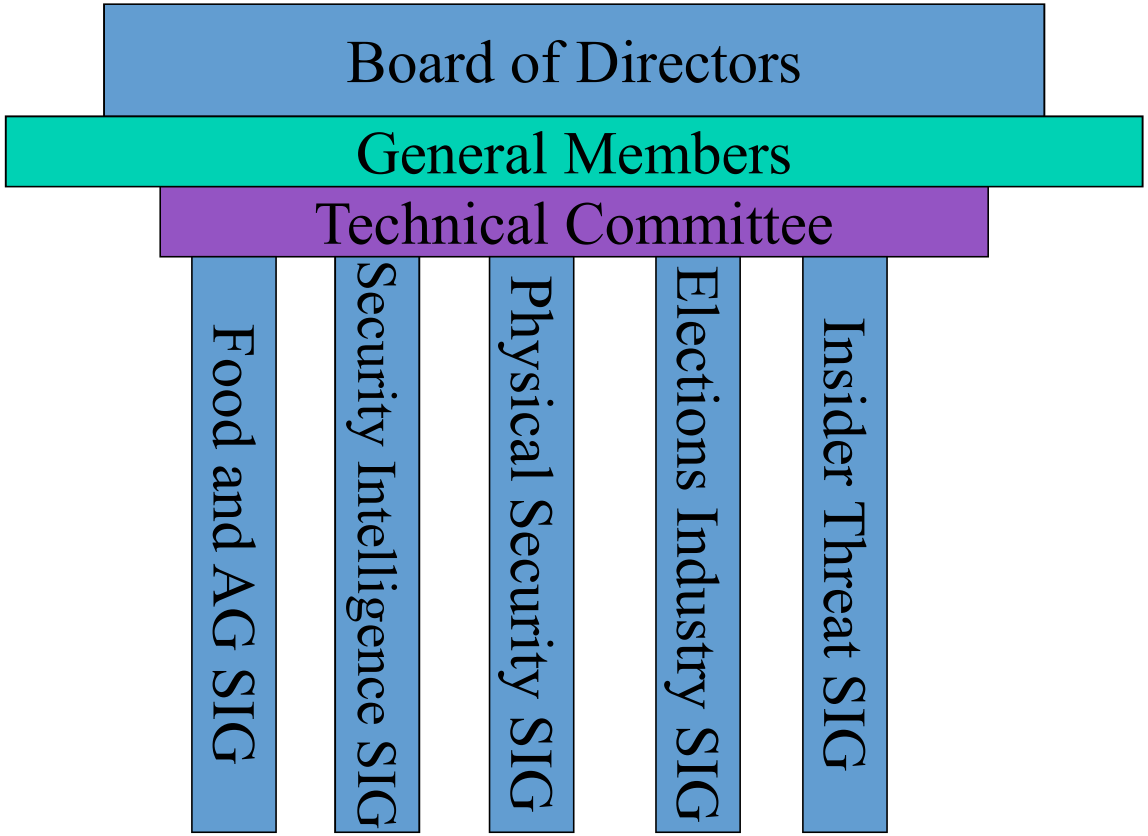
IT ISAC

Information Sharing Relationships



Information Sharing Backbone: TruSTAR

Operational Construct



Board of Directors

General Members

Technical Committee

Food and AG SIG

Security Intelligence SIG

Physical Security SIG

Elections Industry SIG

Insider Threat SIG

Innovate

Provide thought leadership to address pressing operational and policy challenges.

- Pioneered in 2009 a “Functions-Based” approach to sector-wide risk management. This is now the method being applied by DHS through it’s “National Critical Functions” approach.
- Provided road map for joint industry-government operations center. DHS used this to create its cyber operations center.
- Developed and piloted a Concept of Operations for a formal information sharing program among industry and government. This served as the foundation for DHS’ primary industry information sharing program.

Share

Leverage global partners to collect and timely distribute actionable cyber threat indicators, analytical reports and effective practices.

- Partnership with TruSTAR enables members to send and receive information leveraging STIX/TAXII and APIs.
- Make available our Daily Open Source product to the global information security community.
- Through the National Council of ISACs, share and receive information with two dozen additional trusted, information sharing partners.
- Engaging with ICT-ISAC Japan and other organizations to facilitate sharing across borders.

Analyze

Turn information into intelligence that enables members to secure their enterprises.

- IT-ISAC reports provide members tactical and strategic intelligence needed to manage threats to their enterprises.
- Weekly VEAR report provides detailed information on significant but not widely publicized vulnerability exploits.
- Analytic features of TruSTAR platform enables IT-ISAC and members to connect individual indicators to specific incidents, threat actors and campaigns.

Collaborate

Connect analysts from member companies with analysts from peer companies.

- Manage Technical Committee and industry and topic specific “Special Interest Groups” to enable collaboration among members.
- Developed a White Paper highlighting the importance of and impediments to developing Coordinated Vulnerability Disclosure Programs within the elections industry.
- Founder of the National Council of ISACs and IT Sector Coordinating Council, which drive national operational and public policy.
- Active participant in the ISAO Standards Organization’s work to develop practices and guidelines for information sharing organizations.

What's Next

- Celebrating the IT-ISAC's 20th anniversary!
- Develop and promote thought leadership white papers through SIGs.
- Expand Food and Agriculture Special Interest Group
- Enhanced and targeted analytical support to members and partners
  - APT Activity and Vulnerability Reports
  - More reporting on specific incidents
  - Development of joint analytic documents
  - Trends across IT-ISAC Members and Partners

Call to Action

- The threats to our businesses are not sector specific; shared threat is a shared responsibility to respond.

- Drive and influence the development of global information sharing structure by providing thought leadership to policymakers on cyber security and information sharing issues.

- Demonstrate corporate/industry leadership to address pressing national and global security issues on a voluntary basis.

Thank You!!

Scott C. Algeier
Executive Director, IT-ISAC
+1 703-385-4969
salgeier@it-isac.org