THE VALUE OF AN INDUSTRY INFORMATION SHARING FORUM

20TH ANNIVERSARY OF THE
IT-ISAC
FOUNDED 2000

www.it-isac.org

INTRODUCTION

Information Sharing and Analysis Centers (ISACs) were first established as a result of Presidential Decision Directive 63 in 1998. Its main intent was to prevent "physical and cyber-attacks on our critical infrastructures, including especially our cyber systems."[1] The directive encouraged critical infrastructure owners and operators to establish ISACs, to gather, analyze, and share information within critical infrastructure sectors. The ISACs would be a "clearinghouse for information"[2] collecting, aggregating, analyzing, and sharing intelligence regarding vulnerabilities, threats, and other risks.

For this model to be successful, traditional competitors must become collaborators. Over the past 20 years, the IT sector has built and grown an ISAC that has done just this. The IT-ISAC, has helped industry and government respond to the world's most significant cyber-attacks. The IT-ISAC has stood at the forefront of cybersecurity risk management throughout the last two decades, building a trusted community among analysts from the world's leading technology companies, through four key actions - innovation, sharing, analysis, and collaboration.

This paper highlights the importance of information sharing forums like the IT-ISAC, and the value they provide. In doing so, this paper discusses why information sharing forums are crucial, how IT-ISAC value extends beyond information sharing, and why engagement with information sharing forums will remain an important part of corporate security strategies in the future.

AN INFORMATION SHARING FORUM IN THE IT COMMUNITY

The IT-ISAC was founded in 2000 by a small group of leading, US-based companies, and is recognized by the Department of Homeland Security and the IT Sector Coordinating Council as the sector's designated information sharing forum.[3] Today the IT-ISAC's global membership consists of more than 100 industry leaders from three critical infrastructure sectors---IT, food and agriculture, and elections. The premise is simple - collaboration makes everyone stronger. Through trusted collaboration, members can better secure their enterprises and the information infrastructure that propels the digital economy.

---

[1] The White House, "Presidential Decision Directive/NSC-63," May. 1998. Retrieved 16 Feb. 2020 from https://fas.org/irp/offdocs/pdd/pdd-63.htm

[2] The White House, "Presidential Decision Directive/NSC-63," May. 1998. Retrieved 16 Feb. 2020 from https://fas.org/irp/offdocs/pdd/pdd-63.htm

[3] Department of Homeland Security, "Information Technology Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan," May. 2007. p. 40. Retrieved 28 Feb. 2020 from https://www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf

By choosing to participate in an information sharing forum such as the IT-ISAC, members have the benefit of receiving trusted information, analysis, solutions and the ability to enhance cybersecurity across the globe. Collaborating within the IT sector and across sectors is crucial since:

- No company has all the analytical resources it needs. As such, engaging with analysts from peer companies in forums such as the IT-ISAC provides a force multiplier to companies.
- Threat actors are repeating attack methods across victims and across industries.
- Accurate reporting about an active incident or campaign is hard to acquire. ISACs often serve as a "truth detector" helping companies understand the actual scale and scope of incidents.

Lastly, an organization's investment in IT-ISAC membership is minimal compared to the value of the resources and benefits received from membership. For a fraction of the cost of hiring a security analyst, IT-ISAC members supplement their security intelligence and analytic teams by engaging with IT-ISAC staff, collaborating with analysts from leading IT companies, and by leveraging our global network to connect with security experts from around the world.

HOW THE IT-ISAC SHARES

The IT-ISAC provides our members with actionable, timely, strategic and tactical information. To enable this, our goal is to make it as easy as possible for members to send and receive information. For information to be valuable to the membership, they must be able to consume, understand and act based on the information and analysis they receive. Given the wide scale of capabilities among our members, we deploy several tools to ensure we meet each member's needs. For example, we provide timely, high quality threat indicators that members can consume through automation. We have an intelligence management platform that aides our members and team with analysis. We also provide regular threat reporting to members and regular opportunities for members to collaborate. The tools we leverage include:

TruSTAR

TruSTAR, our intelligence management platform, enables us to share indicators at scale and provides context for those indicators as well. The platform gives members access to thousands of threat indicators that are shared by the members, the IT-ISAC operations team, and IT-ISAC industry and government partners. Members can automate the ingest of

feeds through STIX/TAXII integrations and can leverage the user interface for deep dive analytics.

Technical Committee

Technical Committee meetings are led by the IT-ISAC operations team once a week and give members the opportunity to discuss current threats and trends, as well as those that are on the rise. Members and outside experts present on emerging threats, trends, and incidents. Members take the knowledge they gain from these meetings and apply it to defend their companies. The Technical Committee is the main forum used by the IT-ISAC to collaborate on cyber incident response and to share information.

Special Interest Groups

Special Interest Groups (SIGs) enable subject matter experts from across our membership to collaborate on common security topics. SIGs are organized by topic and by industry. The IT-ISAC is unique, as it is the only ISAC that supports three critical infrastructure sectors---IT, food and agriculture, and elections infrastructure. The IT-ISAC currently offers the following SIGs.

- Elections Industry
- Food and Agriculture
- Insider Threat
- Security Intelligence
- Physical Security

Each special interest group operates differently, and their specific goals vary, but they share a common mission to better identify threats within its specific industry or business. One value of the SIGs is that experts within that community can collaborate on projects that will benefit their industry. For example, the Elections-Industry SIG is creating a coordinated vulnerability disclosure program in consultation with experts from the security researcher community. Our Insider Threat SIG is working on a guide that will assist companies who are looking to start an insider threat program.

Secure Messaging Platform

The IT-ISAC uses a secure messaging platform to enable secure collaboration among members. We utilize various channels and stand up additional ones as needed to address specific topics. Since many teams use secure messaging in their companies, analysts are in the habit of using this tool and share frequently and freely within the IT-ISAC Slack channel.

Analytic Reports

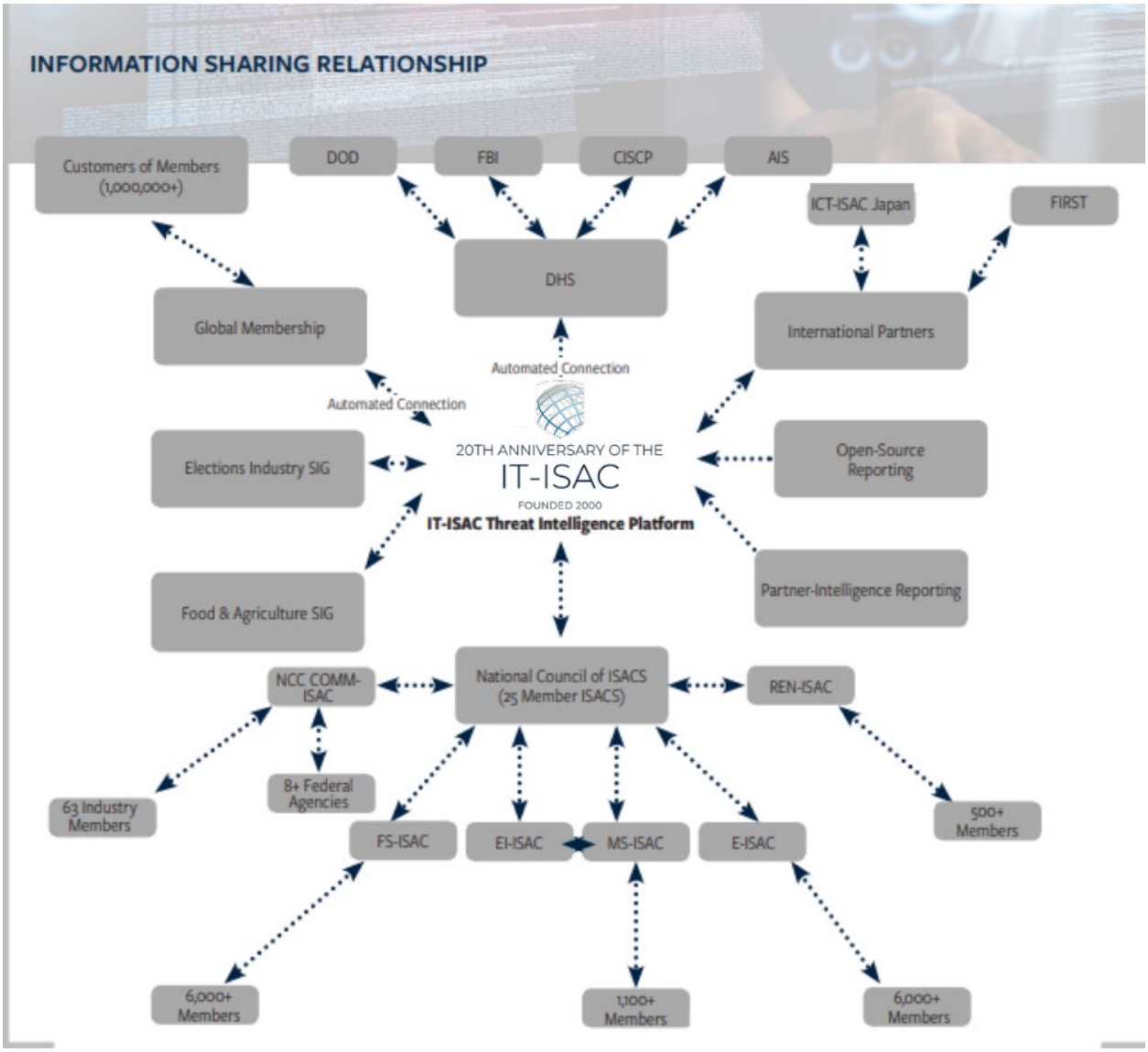
The IT-ISAC has an internal analytic team responsible for developing and sharing threat analysis with members. The primary goal is to help members prioritize what is important and to provide a vendor neutral perspective of high-profile incidents and threats. As such, our operations team produces a daily report that highlights incidents from the previous 24 hours, a weekly report that details important vulnerability exploits, and incident specific reports on high profile attacks, threats, and vulnerabilities. The IT-ISAC also reports on physical security incidents such as terrorist attacks and natural disasters, including COVID-19. These are distributed to members through secure, member only channels.

Additional Information Sharing Relationships

Our two decades of collaboration has enabled us to build a trusted global network. This gives us access to a vast amount of subject matter expertise around the globe and provides us access to information well beyond our immediate membership. We continue to devote a lot of time and attention to maturing and growing these relationships. This includes our relationship with partner ISACs in the National Council of ISACs (NCI). We are also committed to partnering with organizations throughout the world to enhance our common mission.

For example, in November 2019, the IT-ISAC established an operational partnership overseas with the Information and Community Technology-ISAC Japan (ICT-ISAC Japan) and signed a Memorandum of Understanding (MOU). ICT-ISAC Japan is made up of two dozen members that are considered global security leaders, and there are various special interest groups within the organization. The MOU represents a global and collaborative commitment to cybersecurity and showcases the benefit international information sharing can have on critical infrastructure.

The graphic below provides a summary of our trusted global information sharing network. The IT-ISAC is a member of the NCI, which is comprised of 25 ISACs. Many of these ISACs themselves have a global membership base. Collaboration across the ISACs through the NCI is strong, and ISACs share daily with each other. Combined with the collaboration with the NCI and our engagement with organizations such as FIRST and the ICT-ISAC Japan, we have established an effective and robust global reach. We continue to work to expand our global network, but and to also improve it.



BEYOND INFORMATION SHARING

IT-ISAC value extends beyond indicator sharing. A prime value is the ability to collaborate with analysts from peer companies who have experienced (or are experiencing) similar security and business challenges. The IT-ISAC and information sharing forums in general provide a cost-effective way to scale an organization's analytical capability. Instead of being limited to your own team of analysts, an information sharing forum provides you access to analysts from peer companies who face the same challenges.

In the same way, the IT-ISAC has a history of engaging the subject matter expertise within its membership to help address pressing operational and policy challenges. As one example, the IT-ISAC in collaboration with the Communications ISAC first proposed that

DHS integrate its then separate cyber and communications operations centers. A "Tiger Team" comprised of leaders of these ISACs, developed a roadmap that detailed how this could be done. This led to the creation of the National Cyber and Communications Integration Center. Additionally, in 2009, an IT-ISAC led joint industry – government effort pioneered the functions-based approach to sector-wide risk management, detailed in the IT Sector Baseline Risk Assesment.[4] This approach is now being applied by the DHS through its "National Critical Functions" work.

There are additional examples of how the IT-ISAC has applied the subject matter expertise of our members to pressing policy priorities: participating in each of the DHS supported CyberStorm exercises, being part of the team that developed the National Cyber Incident Response Plan, developing with government and partner ISACs to formally integrate the critical infrastructure community into national incident response, engaging the Information Sharing and Analysis Organization (ISAO) Standards Organization to develop effective guidelines and practices that assist newly forming information sharing organizations, and helping to establish organizations such as the IT Sector Coordinating Council and the NCI. The expertise of the IT-ISAC community enables us to add value well beyond information sharing.

THE FUTURE OF INFORMATION SHARING FORUMS

The need for industry specific information sharing forums remains as important today as ever. As cyber threats and technology constantly evolve, it is vital to critical infrastructure that effective mitigation responses and strategies keep pace. IT-ISAC President and BAE Systems Vice President of Intelligence Peder Jungck, recently commented in a blog post that 2020 is the 'age of cyber resiliency.' He lists the necessary steps in being cyber resilient, and specifically calls for more active information sharing. When information is shared about adversaries, companies can better prepare and defend themselves from attacks. When information is not shared, it puts all involved at a disadvantage. "Therefore, information sharing among security operations center is key to helping industry learn all the techniques to protect from a hostile combative landscape and thereby will strengthen infrastructure resiliency."[5]

[4] Department of Homeland Security, "Information Technology Sector Baseline Risk Assessment," Aug. 2009. p. 21. Retrieved 20 Apr. 2020 from https://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf

[5] Peder Jungck, "Welcome to 2020: The Age of Cyber Resiliency," LinkedIn, *Peder Jungck,* Feb. 2020. Retrieved 16 Feb. 2020 from https://www.microsoft.com/security/blog/2015/01/29/info-sharing-testimony/

CONCLUSION

As the IT-ISAC celebrates 20 years of collaborative information sharing and analysis, it is right that we take stock of all that we have achieved. However, when it comes to cybersecurity, if you are not moving forward you are moving backwards. Therefore, we are committed as we were 20 years ago to engaging with members and partners to continue to grow a global network of trusted information security forums. The scope of the cyber threat requires nothing less.

20TH ANNIVERSARY OF THE IT-ISAC
FOUNDED 2000

THE VALUE OF THE IT-ISAC

COLLABORATION

Membership in the IT-ISAC provides your company with the opportunity to engage with 100 leading technology companies across three critical infrastructures who leverage technology for their core business functions through a listserv, secure messaging platform, the IT-ISAC team, regular member calls, and TruSTAR, our intelligence management platform.

ANALYSIS

Members receive analysis through daily trending reports, incident specific-reports, and our VEAR report. Members can also leverage internal analytics within the platform, and pull indicators from TruSTAR into their internal tools.

THOUGHT LEADERSHIP

The IT-ISAC supports advancing cybersecurity through industry-government partnerships. We also enagage with global thought leaders on public policy issues dealing with cybersecurity, specifically information-sharing issues.

Examples of IT-ISAC Collaboration:

- *Member A receives a potential ransomware email. The IT-ISAC contacts its members and other ISACs and learns another organization received a similar message and can conclude it is a hoax.*
- *Member B shares with the membership they have seen an IP address from a hostile nation. The IT-ISAC team distributes the suspicious IP to members, collects responses, collaborates and shares feedback with all members, including the one that submitted the original RFI.*
- *Member C shares they have a big data integration project, and share the problems they are dealing with. Fellow IT-ISAC members offer their experience implementing similar projects. They share strategies that worked, did not work, and things to avoid. Their guidance helps Member C implement their big data integration project with additional knowledge and confidence.*

Examples of IT-ISAC Analysis:

- *Our member-only Daily Cyber Report highlights incidents and threats from the previous day, while our Weekly Cyber Report details impactful vulnerability exploits.*
- *Our Vulnerability and Exploitation Action Report (VEAR) provides detailed analysis on active but under reported vulnerability exploits.*
- *Through trusted collaboration with partner ISACs and government, we receive and share analytic reports from other ISACs and security vendor partners.*

Examples of IT-ISAC Involvement in Thought Leadership:

- *Created the road map for a joint-industry government operations center which is now the DHS National Cybersecurity and Communications Integration Center (NCCIC).*
- *Pioneered the "functions based" approach to sector-wide risk management, which is now being applied by DHS through its "National Critical Functions" approach.*
- *Drove industry collaboration with DHS to ensure industry is integrated in national risk management and incident response frameworks.*
- *Helped to establish organizations such as the IT Sector Coordinating Council + the National Council of ISACs.*