EXECUTIVE SUMMARY

2020 will undoubtedly be remembered for COVID-19. However, 2020 also marked the 20th Anniversary of the IT-ISAC. Despite the uncertainties, disruptions, and havoc unleashed by the pandemic, the Information Technology-Information Sharing and Analysis Center experienced one of its most successful years. We helped members understand and navigate new threats posed by COVID-19, improved and introduced new analytic reports, forged partnerships across the globe, increased membership at a record rate, and expanded our marketing and communications program. 20 years after our founding, the IT-ISAC is well-positioned to not only weather the COVID-19 disruptions but to continue to expand capabilities and services, adding additional value to members and ensure we continue to meet our core mission of serving as a collaborative, trusted forum, that enables members to better manage enterprise risks.

OPERATIONS AND ANALYTICS

At our core, the IT-ISAC is an operational organization. We collect, analyze, aggregate, and share curated threat information that enables members to take informed actions to enhance the security and resiliency of their enterprises. We provide a trusted forum in which members can share and collaborate on common threats. As such, a key focus of the organization is building and maintaining operational capabilities that meet the unique needs of our members.

2020 produced a wide range of cyber threats. Although we have been monitoring and reporting on the Ransomware threat for a while, 2020 saw an increasing number of destructive Ransomware attacks in government and industry networks across the globe. COVID-19 expanded the attack surface and introduced new security challenges. Of course, 2020 was also a presidential election year, and protecting the election from cyber threats was a priority for the government and our Elections Industry Special Interest Group. All this in addition to numerous zero-day vulnerabilities, several vulnerabilities with a CVSS score of 9.8 or higher, and various nation state campaigns, the most high profile of these being the SolarWinds supply chain attack.

The challenges facing the IT-ISAC and our members were never greater, but our response to these challenges was even stronger.
Reports

To help members stay informed of these threats, the IT-ISAC Operations Team produces various reports for our members including a Daily Report that highlights and links to key security incidents, events, and vulnerabilities, a Weekly Report that highlights significant reports from throughout the week, a weekly Vulnerability and Exploitation Report (VEAR) that shares technical analysis on active exploits that are public, but underreported, breaking news reports that summarize major cyber incidents, and quarterly trending malware reports that highlight the most prevalent malware strains currently impacting the IT sector. Below is a sampling of some of our reporting:

Notable IT-ISAC Incident Response Updates in 2020

- 1-14-2020 - Critical Vulnerabilities in Microsoft Windows Operating Systems
- 3-9-2020 - Threat Actors Scan Internet for Vulnerable Microsoft Exchange Servers
- 3-11-2020 - Wormable Windows SMBv3 CVE-2020-0796 Flaw
- 3-24-2020 - Microsoft Warns of Hackers Exploiting Unpatched Windows Bugs
- 7-5-2020 - F5 Releases Security Advisory for BIG-IP TMUI RCE - CVE-2020-5902
- 7-14-20 - SAP Netweaver AS Java - CVE-2020-6287
- 7-16-20 - 'Wormable' RCE Vulnerability in Windows DNS Server - CVE-2020-1350
- 9-1-2020 - CVE-2020-3566 - Cisco Releases Security Advisory for DVMRP Vulnerability in IOS XR Software
- 10-29-2020 - CVE-2020-1472 Active Exploitation
- 11-3-2020 - VMware - CVE-2020-4006
- 12-14-2020 - SolarWinds Orion Code Compromise

Notable White Papers from 2020

Our team produced three notable white papers in 2020.

- Quarter 2 Trending Malware Report - Highlighted the most prevalent malware strains impacting the IT sector. The list of malware strains we included in this report was developed in collaboration with our membership, who helped identify which malware strains were most commonly seen in attacks. The distribution of this white paper was limited to our members and public and private sector partners.
• **COVID-19 Challenges and Lessons Learned Report** - Documented cybersecurity challenges experienced by companies because of the mass transition to remote work due to COVID-19. This publicly shared paper also offered lessons learned, incorporating input from both our own members and independent, public sources.

• **The Value of an Industry Information Sharing Forum** - Discussed 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. This paper was shared with the public.

**Technical Committee**

We hold a weekly Technical Committee Meeting that provides members the opportunity to receive briefings on current and emerging cybersecurity issues and trends. As part of our onboarding process, all IT-ISAC members are added to our Technical Committee listserv. This listserv is the channel through which IT-ISAC members receive reports from our Operations Team and updates from our Organizational Team. The Technical Committee also receives presentations from subject matter experts. Our 2020 guest presentations include:

- January 21, 2020 - Mimecast - CVE-2019-1463
- February 18, 2020 - TrendMicro - IoT Honeypot
- March 24, 2020 - ESET - Kr00k Vulnerability
- April 27, 2020 - Insider Threat SIG - Where Should Insider Threat Program Reside
- May 26, 2020 - IBM - Detecting Nation State Attacks
- July 7, 2020 - Cycognito - Attack Surface Monitoring
- August 4, 2020 - McAfee - COVID-19 Threat Report
- August 11, 2020 - SpyCloud - Account Takeover Statistics
- November 17, 2020 - CompTIA - Member Benefits Overview
- December 1, 2020 - CrowdStrike - Derick Buchanan
- December 8, 2020 - ISACA - Member Benefits Overview

**Special Interest Group Updates**

**Food and Agriculture SIG**

Our Food and Agriculture Special Interest Group provides a forum for our members in the Food and Agriculture industry to share information on common security threats and collaborate on effective mitigations. The SIG shares information via twice a month virtual meetings and a dedicated enclave in TruSTAR, the IT-ISAC’s intelligence management platform.
Early in 2020, the IT-ISAC entered into an agreement to collaborate with Auburn University, thanks to the leadership of Dr. Robert Norton, Professor of Veterinary Diseases, Biosecurity, and Public Health at Auburn University. IT-ISAC Executive Director Scott Algeier also co-authored pieces with Dr. Norton for *Food Safety Magazine*, which highlighted why cybersecurity in the food and agriculture industry is both a business security and a national security concern. Our work with Dr. Norton has been somewhat disrupted due to COVID-19, but we look forward to getting back on track in 2021.

We are also pleased to have established a relationship with Dr. Susan Duncan from Virginia Tech University. Dr. Duncan is the Associate Director of the Virginia Agricultural Experiment Station at Virginia Tech. Dr. Duncan participated in a *FireWall Chats* podcast with Dr. Norton and IT-ISAC Operations Manager Jonathan Braley to discuss threats to the food and agriculture sector.

**Elections Industry SIG**

2020 also marked the two-year anniversary of the Elections Industry Special Interest Group. The SIG supports voting technology providers by providing them an industry-only forum to share information threats to their enterprises and systems, and to collaborate on challenges facing the industry. Since its formation, the SIG has focused on building Coordinated Vulnerability Disclosure Programs within the industry. Some highlights from 2020 include:

- **February 2020** - Established an Advisory Committee to continue the group's efforts on developing corporate coordinated vulnerability disclosure programs.
- **July 2020** - Security researcher and advisory committee member Jack Cable participated in an IT-ISAC FireWall Chats podcast.
- **August 2020** - EI-SIG Two Years of Progress White Paper was published, EI-SIG members continued to develop and finalize their corporate CVD programs, showcased on the IT-ISAC website.
- **October 2020** - IT-ISAC Executive Director Scott Algeier moderated a HackerOne Security@Conference session on the role hackers can play in protecting to protect election systems, with some of our SIG and its Advisory Committee members on the panel.

**Insider Threat SIG**

Our Insider Threat SIG continues to meet bi-weekly. The SIG is designed for those who are responsible for building and managing Insider Threat programs within their companies. In addition to helping members manage insider threats, the SIG spent a lot of time in 2020 working on an Insider Threat Starter Guide.
The guide will leverage the combined expertise of SIG members to create a usable document for the rest of the membership. This guide is expected to be released to members in Q1 2021.

**Physical Security SIG:**

Our Physical Security SIG is composed of security and business continuity professionals from our member companies. Throughout the year, we shared numerous CISA and other public and private sector partner reports on COVID-19, hurricanes, wildfires, other natural disasters, and physical security attacks with the SIG. We also uploaded these reports to our private Physical Security SIG Slack channel.

**Operations Working Group**

To ensure the IT-ISAC continues to meet the needs of members in the year ahead, we formed a working group of members to evaluate our technological needs, analytical gaps, and establish operational priorities based on identified needs and gaps. This group has proposed ways to enhance our operations and is informing investment decisions by the Board.

Working with the group, we were able to highlight the following operational requirements:

- **Tactical Intelligence/Situational Awareness**
  - What the IT-ISAC is doing to help members respond to incidents

- **Strategic Intelligence**
  - What the IT-ISAC is doing to help members defend themselves and to improve their overall cybersecurity posture

- **Incident Analysis**
  - How the IT-ISAC is raising awareness of cybersecurity incidents to members

- **Threat Intelligence**
  - What the IT-ISAC offers to help members manage threats

- **Historical Knowledge Repository**
  - Secure collaboration and document storage portal

**Cybersecurity Awareness Month**

November 2020 marked the 17th Anniversary of National Cybersecurity Awareness Month. This year's theme was, "Do Your Part. #BeCyberSmart." The IT-ISAC once again supported this important initiative by becoming a Cybersecurity Awareness Month champion and sharing helpful tips on how to be cyber smart on social media.
We also published a blog post called, "Simple Solutions for a Complex Threat," that sought to bring awareness to today's threat landscape, and recommended actions end users should take to secure their part of cyberspace.

IT-ISAC Operations Manager Jonathan Braley and Operations Coordinator Ian Andrieckack also participated in Cybersecurity Awareness Month with one of our members, CDK Global. Ian and Jonathan presented to CDK employees on recent phishing campaigns, how COVID-19 has changed the attack surface and offered best practice tips on avoiding phishing attacks.

MEMBERSHIP

New Members

We welcomed 30 new members to the IT-ISAC in 2020--13 bronze, 12 silver, and five gold level members. The five new Board member companies are Carrier, Corteva, Ingram Micro, Qualys, and Veeam. These new member companies represent a multitude of industries including food and agriculture, elections, IT, machinery, HVAC, marketing, cloud computing computer software, ridesharing, technology, manufacturing, cybersecurity, law, software, insurance, and communications. The IT-ISAC's membership reflects the diversity of the IT industry and our mission to support three critical infrastructure sectors--IT, Food and Agriculture, and Elections.

PARTNERSHIPS

The IT-ISAC recognizes that cybersecurity is an issue of global concern and it is of utmost importance that organizations build partnerships beyond their organizations, sectors, and national boundaries. To achieve the best risk management, and to manage the negative consequences of a successful cyberattack, requires trusted communication and cooperation to decrease and eliminate threats, risks, and vulnerabilities. Part of our mission is to serve as a force-multiplier that enables collaboration and sharing of relevant and actionable cyber threat information. The following operational partnerships are designed to help us meet that mission.

Auburn University

As noted, early in 2020 we established a partnership with Auburn University to collaborate on issues related to cybersecurity in the Food and Agriculture industry.
Cyber Threat Alliance

In May we announced a working agreement with the Cyber Threat Alliance to cooperate on threat intelligence and coordinate during cybersecurity incidents and emergencies. CTA and the IT-ISAC will engage in analytical exchanges on specific threats, trends, cyber incidents, reports, and research of mutual interest.

CompTIA ISAO

We partnered with TruSTAR and the CompTIA ISAO to provide an intelligence exchange and reporting for the ISAO to serve as the focal point for dealing with cyber threats to technology vendors, MSPs, solution providers, integrators, distributors, and business technology consultants. As part of this agreement, the IT-ISAC also provides operations and analytic support services to the ISAO.

TruSTAR

TruSTAR provides the IT-ISAC a consistent way to share indicators at scale. It also enables members to easily integrate TruSTAR with their internal security tools and to leverage capabilities within TruSTAR to conduct analysis on IoCs. Members likewise use TruSTAR to share information with each other. To provide consistency and stability within the IT-ISAC Operations and with our members, in 2020 we announced the renewal of our partnership with TruSTAR to serve as our intelligence management platform.

Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC)

In October we signed an MOU with the Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC). This strategic partnership allows both organizations to provide new sources of information to each other, enable direct collaboration on threats and incidents as needed, and expand the visibility and branding of the IT-ISAC and TWCERT/CC. Additionally, when appropriate, both organizations will share open-source intelligence, malware analysis, and incident alerts or threat warnings.
EDUCATION AND TRAINING

In 2020, we also made progress on addressing a long-standing need for many of our members, which is to help ensure employees have the cyber skills they need. We did this by partnering with leading providers of training and certifications to provide discounted rates to IT-ISAC members and their employees.

CompTIA

Through our partnership with CompTIA (supporting the CompTIA ISAO), the following discounts are offered to our members:

- 15% off CompTIA corporate and ISAO membership
- 15% off CompTIA training and certification products

EC-Council

In November, we signed a Memorandum of Understanding with the EC-Council. Through this partnership, our members receive exclusive discounts on EC-Council's highly respected certification programs.

- EC-Council Benefits for IT-ISAC Members:
  - Discounts on the following EC-Council training programs and workshops:
  - Certified Ethical Hacker (CEH)
  - Computer Hacking Forensics Investigator (C|HFI)
  - Certified Security Analyst (ECSA)
  - Certified Network Defender (CND)
  - STORM Workshop

ISACA

In November we announced the formation of a strategic partnership with ISACA. The partnership is focused on providing additional cybersecurity thought leadership to ISACA members and on expanding training and education to technology and cybersecurity professionals.
ISACA Partnership Benefits for IT-ISAC Members:

- ISACA Membership Rates on the following:
  - CSX Technical Foundation Series Bundle - $500
  - CSX Penetration Test Course - $275
  - CSX Emerging Technology Specialist Pathway - $500
  - CSX-P Cybersecurity Practitioner Certification Suite - $800
  - CISM Certification, Certification Exam - $575, QAE & Review Manual - $475
  - CRISC Certification, Certification Exam - $575, QAE & Review Manual - $405

COMMUNICATIONS & MARKETING

The IT-ISAC seeks consistent, sustained year-over-year growth without disrupting our trust model. Organizational growth enables us to invest resources to support members. The key to this is implementing a communications and marketing strategy that promotes organizational successes and value.

We constantly seek to establish brand recognition amongst our audiences and ultimately, recruit and retain members. Of course, we also seek to consistently keep our members and other audiences up to date on our work, engage with our members, and provide new information to our members through our communications and marketing initiatives. Some important initiatives and campaigns we completed in 2020 are:

20th Anniversary

In January, we kicked off our 20th Anniversary campaign. We unveiled a new organizational logo and a 20th Anniversary logo, published an updated membership brochure, and a 2020 Fact Sheet. We also revamped the look of the website to match the new organizational colors and theme and ran a fact of the week campaign on social media to share all that we've accomplished over the last 20 years, in addition to general information about the ISAC.

Podcasts and Blogs

Podcasts and blogs provide us with an opportunity to promote thought leadership and visibility on key issues. In 2020, we expanded these initiatives.
January - **FireWall Chats: Episode 6** - **Robert Norton**, Auburn Professor of Veterinary Infectious Diseases, Biosecurity, and Public Health in the College of Agriculture, and Director of the Futures Laboratory, FireWall Chats: Episode 7 - Pt. 1 - **Guy Copeland**, Former IT-ISAC Founding Board Member and President

February - FireWall Chats Blog Post: "**AIS and the Original CISA: A Review of Cyber Threat Information Sharing**"

March - FireWall Chats: Episode 7, Pt. 2 - Guy Copeland, Former IT-ISAC Founding Board Member and President

July - FireWall Chats: Episode 8 - Jack Cable, Security Researcher and EI-SIG Advisory Committee Member

August - FireWall Chats: Episode 9 - Larry Clinton, Internet Security Alliance President, FireWall Chats: Episode 10, Pt. 1 - Eric Coomer, Sam Derheimer, and Brian Hancock, EI-SIG Members


October - FireWall Chats Blog Post: "**Simple Solutions for a Complex Threat**"

November - FireWall Chats: Episode 11 - MJ Shoer, CompTIA ISAO Executive Director

December - FireWall Chats: Episode 12 - Susan Duncan, Ph.D., Robert Norton, Ph.D., and Jonathan Braley

**Social Media**

**Twitter**

In 2020, the IT-ISAC gained 285 new followers. We currently have 1,890 followers. In 2020, our tweets received 240.2K impressions and users visited our profile 4,593 times. We tweeted 129 times in 2020.
LinkedIn

We gained **512** new LinkedIn followers in 2020. We currently have **951** LinkedIn followers. In 2020, our updates received **23,819** impressions, and users visited our profile **2,062** times. We posted 116 LinkedIn updates in 2020.

YouTube

In February, we created a YouTube channel and published the IT-ISAC’s first-ever video, "**We are the IT-ISAC**." The YouTube channel provides a different form of content for our members, prospective members, and other audiences. It also creates more visibility for the IT-ISAC and enables us to promote the value of the IT-ISAC in different video formats, as demonstrated by our "**The Value of the IT-ISAC**" video.

Also, while we still upload our podcasts to Soundcloud in audio form, we upload a video format on our YouTube channel as well, which has provided great visibility. It allows us to engage with our members and partners on another social media platform. We have utilized our channel to post weekly updates from our Operations Team about incidents from the week and provide guidance on how to best mitigate current threats our team has seen.

The IT-ISAC has **1,070** subscribers. In 2020, our channel was viewed **29,630** times, and our videos received a total of **29.6K** views. We have published 12 public videos on our channel.

Videos:

- **February** - We are the IT-ISAC
- **April** - The Value of the IT-ISAC
- **June** - TruSTAR Tutorial Series
- **July** - FireWall Chats: Episode 8 - Jack Cable, File Hashing Demonstration, Unsung Cyber Hero Adventures TV Network Interview with IT-ISAC Executive Director
- **August** - FireWall Chats: Episode 9 - Larry Clinton, FireWall Chats: Episode 10, Pt. 1 - Eric Coomer, Sam Derheimer, and Brian Hancock
- **September** - FireWall Chats: Episode 10, Pt. 2 - Keir Hollman, Ed Smith, and Chris Wlaschin
- **November** - FireWall Chats: Episode 11 - MJ Shoer
- **December** - FireWall Chats Episode 12, Pt. 1 - Susan Duncan, Ph.D., Robert Norton, Ph.D., and Jonathan Braley
Media and Thought Leadership Engagements

January - Scott spoke at the Pacific Telecommunications Council Annual Conference about the IT-ISAC's partnership with the ICT-ISAC Japan.

February - Scott and Auburn University's Dr. Robert Norton co-authored a piece featured in Food Safety Magazine called, "Food and Agriculture Are Critical Infrastructures but also Domains of War."

April - Food Safety Magazine published another article written by Scott and Auburn University's Dr. Norton titled, "Food Defense is All About Protecting Yourself."

May - We announced the signing of a working agreement with the Cyber Threat Alliance to cooperate on threat intelligence and coordinate during cybersecurity incidents and emergencies.

June - Synack hosted a webinar with their CEO Jay Kaplan and IT-ISAC President Peder Jungck, to discuss how companies are prioritizing security solutions to create a lean security budget in the COVID era.

July - Scott was interviewed by Gary Berman, host of the Unsung Cyber Hero Adventures TV Network.

August - Scott was the opening speaker at the 3rd Annual Managed Security Services Forum San Diego. He discussed COVID-19's impact on cybersecurity and the need for cybersecurity collaboration.

September - We announced the renewal of our partnership with TruSTAR and our partnership with the CompTIA ISAO to provide intelligence exchange and reporting for the ISAO. On Sep. 30, Scott and CompTIA ISAO Executive Director MJ Shoer spoke at the 4th Annual International Information Sharing Conference hosted by the ISAO Standards Organization about the value of collaboration between information sharing forums and how these serve as an effective cost-multiplier for organizations.

October - The CyberWire published a podcast featuring Scott, where he discussed how information sharing has evolved over the last 20 years.
On Oct. 20, Scott moderated a panel discussion at HackerOne's Security@ Conference about the role hackers play in helping protect election systems. On Oct. 29, IT-ISAC Operations Manager Jonathan Braley joined Mj Shoer on a LinkedIn live to discuss threats detected by the ISAO and what they mean for technology business leaders.

**November** - Scott joined MJ on an episode of his talk show, *Shoering Up Security*, to discuss how we’re working with the CompTIA ISAO to provide critical threat intelligence and improve the cyber resiliency of the IT industry. Also in November, Scott participated in the FIRST Annual Conference as a panelist with other ISAC representatives to discuss the role of ISACs. On Nov. 10, Scott spoke at the Second Annual Managed Security Services Forum Miami. On Nov. 19, we announced our strategic partnership with ISACA to provide additional cybersecurity thought leadership to ISACA members and expand training and education to technology and cybersecurity professionals. On Nov. 24, we announced that we signed an MOU with EC-Council. The partnership allows for IT-ISAC members to receive exclusive discounts on EC-Council’s certification programs and the cross-promotion of both organizations’ cybersecurity initiatives and content.

**December** - Scott contributed an article to ISACA's newsletter, *The Nexus*, called, "Why You Need to Take Cybersecurity Seriously in the New Year." The article talks about what shapes today's threat landscape and the importance of organizations being proactive about cyberthreats.

**Public Policy Engagements**

While the IT-ISAC is primarily an operational organization, we do provide thought leadership on cybersecurity and information sharing policy. The IT-ISAC does not lobby and does not advocate for any specific legislation. Instead, we engage through established public-private partnership structures.

**DHS Supply Chain Risk Management Task Force** - The IT-ISAC is a voting member of the ICT Supply Chain Risk Management Task Force. The task force is tasked with “identifying and developing consensus strategies that enhance ICT supply chain security.” In December, the task force released its Year Two report.

**Cyber Threat Information Sharing Working Group** - Scott is an industry Co-Chair of this Critical Infrastructure Protection Advisory Council (CIPAC) working group focused on improving information sharing between DHS, CISA, industry, and state, local, tribal, and territorial governments.
**National Infrastructure Plan Refresh Working Group** - This working group is focused on updating several sections of the National Infrastructure Protection Plan, which was last updated in 2013.

**National Critical Functions** - DHS and CISA continue to implement an approach to identify and manage risks to core functions that propel the economy and are vital to national security. This "critical functions" approach was developed by a working group the IT-ISAC Chaired from 2007 - 2009. The IT-ISAC continues to engage in this work through the IT Sector Coordinating Council’s dedicated working group.

**CONCLUSION**

Despite the ongoing challenges of the pandemic, the IT-ISAC achieved quite a lot in 2020. We were able to grow our membership, expand and enhance our operations, and established partnerships with leading organizations, including three leaders in IT training and certification. We also successfully implemented a 20th Anniversary campaign, celebrating two decades of information sharing and collaboration, and were able to widely communicate the value of the IT-ISAC by growing our social media portfolio. We are excited about the future of the IT-ISAC and look forward to continuing this success into 2021 and beyond.
2020 IN REVIEW

30 NEW MEMBERS
12 THOUGHT LEADERSHIP ENGAGEMENTS
11 TECHNICAL COMMITTEE GUEST SPEAKERS INCIDENT REPORTS FIREWALL CHATS BLOGS & PODCASTS
5 NEW CYBER PARTNERSHIPS

4 EI-SIG MEMBERS PUBLISHED CVD PROGRAMS PUBLIC POLICY ENGAGEMENTS
3 NEW EDUCATIONAL PARTNERSHIPS WHITE PAPERS
2 FOOD AND AGRICULTURE SIG PARTNERSHIPS
1 EI-SIG PROGRESS REPORT