InfoSec Summit 2022

Information Sharing: Where do I start and how do I get the approval to do this?

Errol Weiss
Health-ISAC Chief Security Officer

SHARING SINCE 2010
H-ISAC®
HEALTH - ISAC

Updated 07.27.2022

What is an ISAC?

- ISAC is short for “Information Sharing and Analysis Center”
- ISACs empower **sharing and collaboration** in critical infrastructure communities to prevent, detect and respond to cybersecurity and physical security events
- ISACs collect, analyze, and disseminate actionable **threat information** to their members and provide them with **tools** to mitigate risks and enhance resiliency

national council of
ISACs
MEMBER ISAC
AUTO-ISAC
AVIATION ISAC
E-ISAC
Cyber Share
DNG-ISAC
Elections Infrastructure ISAC
FS-ISAC
MARITIME ISAC
MEISAC
MS-ISAC
REN-ISAC
RETAIL & HOSPITALITY ISAC
H-ISAC
Real Estate ISAC
WATER ISAC
IT-ISAC
ONG-ISAC
SPACE ISAC
NCC

About Health-ISAC

- Community of Global Security Analysts, built on **trust** and **anonymity**
- Members are in the health sector and interested in providing value to the overall Health-ISAC eco-system by listening, sharing, and/or contributing

Johnson & Johnson

MERCK

McKESSON

Takeda

AMGEN

Pfizer

DANAHER

Lilly

Hospitals

Insurance (Payers)

Academic Medical Schools

Medical Device Manufacturers (MDM)

Electronic Medical Records (EMR)

Group Purchasing Organizations (GPO)

Pharmaceutical

Pharmacies

Telehealth

Laboratories

Radiological Centers

Revenue Cycle Management

Healthcare Supply Chain

Mortuaries

R&D Centers

Hospice

Clearing Houses

Community

- Connect with 7,000+ Security Analyst peers anonymously and in real-time using:
  - End-to-End Encrypted Chat
  - Listserv
  - Member Surveys
  - Networking Support
  - Working Groups, Committees, and Councils

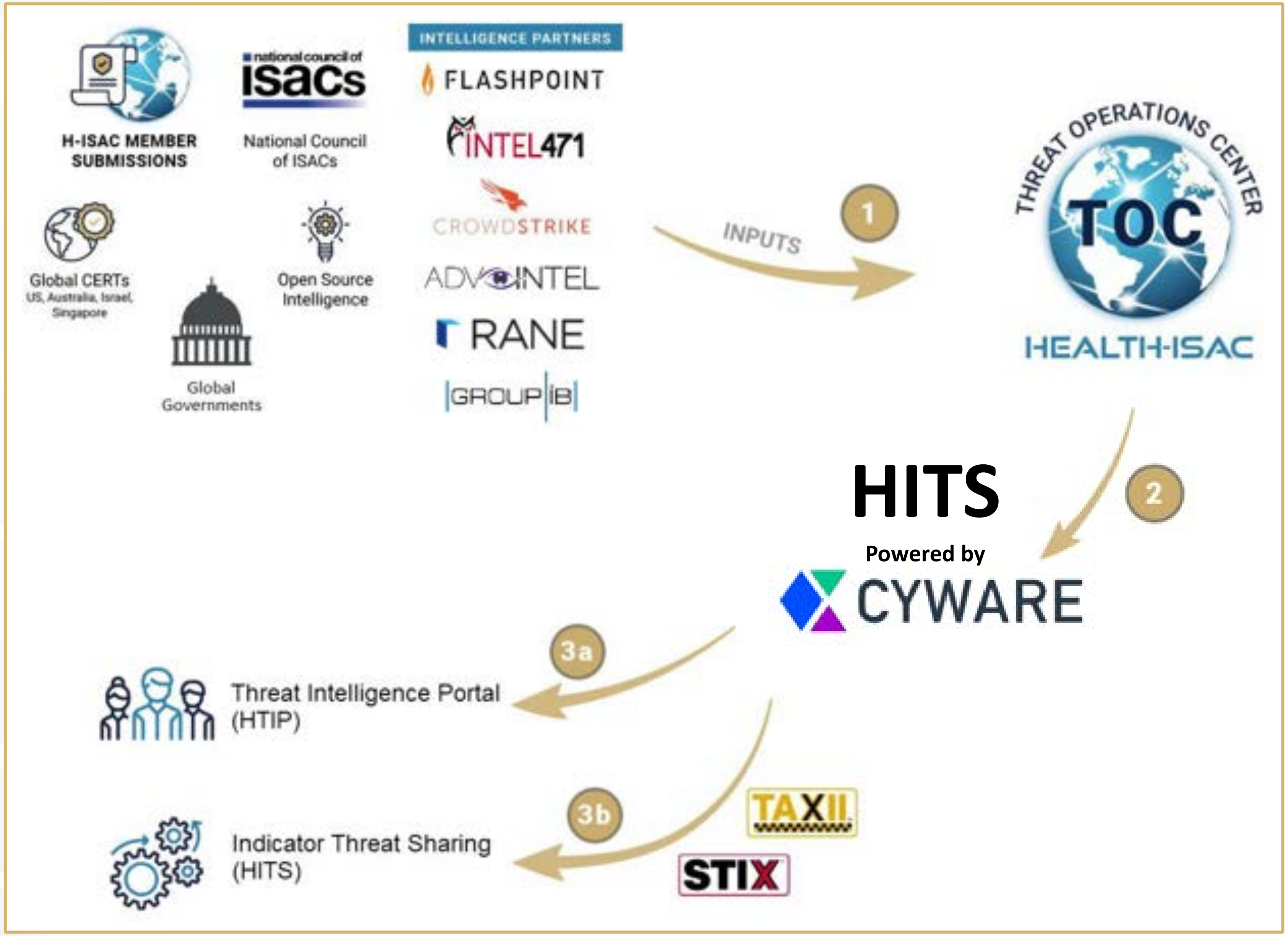
Medical Device Security Information Sharing (MDSISC)
Business Resilience
Cyber Threat Intelligence Program Development
Cybersecurity Analytics
Cybersecurity Awareness and Training
Diversity and Inclusion
European Council
Identity and Access Management (IAM)
Third Party Risk Governance (TPRG)
Insider Threat
Pharma and Supply Chain
IT M&A Integration and Divestitures
Provider Special Interest Group
Purple Teams

Threat Intelligence

- **Threat Operations Center (TOC)** – Analysts on staff who deliver:
  - Targeted Alerts
  - Threat/Vulnerability Bulletins
  - Daily Cyber Headlines
  - Dark Web Monitoring
  - Monthly Threat Brief (MTB) Webinars
  - Pre-Public Alerts
  - Global Cyber Threat Level Botnet Disruption
  - Microsoft Patch Tuesday Podcast w/ Microsoft Cybersecurity Expert

CYBER THREAT LEVELS
SEVERE
SEVERE RISK OF CYBER ATTACKS
HIGH
HIGH RISK OF CYBER ATTACKS
ELEVATED
SIGNIFICANT RISK OF CYBER ATTACKS
GUARDED
GENERAL RISK OF CYBER ATTACKS
LOW
LOW RISK OF CYBER ATTACKS
H-ISAC

Automated Threat Intelligence & Cybersecurity

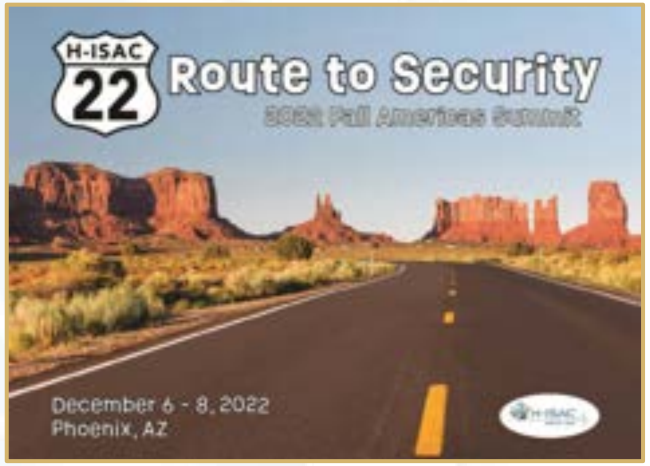


Indicator Threat Sharing (HITS)

- Automated collections of Indicators of Compromise (IOCs) sent directly to SIEM, endpoint protection, or data warehouse. (powered by Cyware)
  - Member provided IOCs
  - Vetted by the TOC to limit false positives

"In the last 7 days, 22.92 million blockings are attributable to the Health-ISAC Amber Members list with zero false positives – and we have never received a reported false positive from the list."

Events & Education



Summits

Fall Americas (West)

Spring Americas (East)

European

APAC

Workshops and Webinars

Tabletop Exercises (TTX) and After-Action Reports

Cyber Threats Impacting the Healthcare Sector (July 2022)

- Ongoing targeted social engineering attacks
  - Directed at service/help desk call centers to obtain confidential information
  - Threat actors leverage personally identifiable information (PII)
  - Bypass rudimentary security checks
  - Health-ISAC recommends members review and harden call center policies
- Raccoon Stealer
  - Members report attempts to deliver credential stealing malware
  - The malware-as-a-service (MaaS) threat has returned

CYBER THREAT ADVISORY
GUARDED
GENERAL RISK OF CYBER ATTACKS
H-ISAC

A threat of increased cyber activity exists stemming from general events or threats. Additional defensive actions may be assumed against the general threat or event.

Cyber Threats Impacting the Healthcare Sector (July 2022)

- Brute Ratel
  - A cyber security / hacking toolkit like Cobalt Strike
  - Threat actors have been observed abusing its capabilities and C2 infrastructure in malicious operations
- Callback campaigns
  - Threat actors ate impersonating reputable cybersecurity firms to socially engineer victims
  - Gain access via legitimate remote access tools like TeamViewer and PC Anywhere
  - Malicious actors deliver emails with apparent urgent issues and a phone number for the victim to call
  - Emails contain no links or malicious files

Booz | Allen | Hamilton

H-ISAC
HEALTH · ISAC

February 2022

Current and Emerging Healthcare Cyber Threat Landscape

This report is a collaboration between Health-ISAC and Booz Allen Hamilton Cyber Threat Intelligence (CTI).

TLP:GREEN Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community.

TLP:GREEN information may not be released outside of the community.

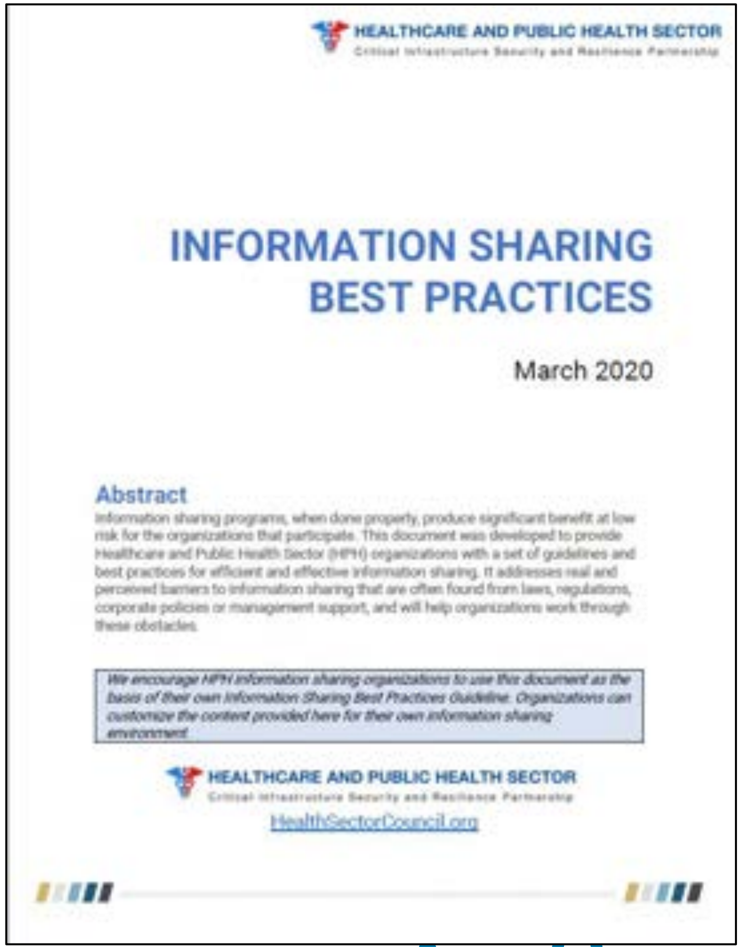
-isac.org

https://h-isac.org/health-isacs-first-annual-current-and-emerging-healthcare-cyber-threat-landscape-executive-summary/

Information Sharing Makes It All Happen

Information Sharing Best Practices

- Health Sector Coordinating Council
  - Public / Private Partnership
  - Published on March 11, 2020
- What is the Information Sharing Best Practices Guide?
  - Guidelines and best practices
  - Address real and perceived barriers to info sharing
  - Navigate challenges from laws, regulations and corporate policies
  - Gain management support
- Use the document as the basis of your own internal Information Sharing Best Practice / Policy
- Feedback is encouraged
- Intended to be a “living document” with frequent updates
- Information Sharing Best Practices White Paper / Toolkit
  - https://h-isac.org/h-isac-information-sharing-best-practices/



HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership

INFORMATION SHARING
BEST PRACTICES

March 2020

Abstract

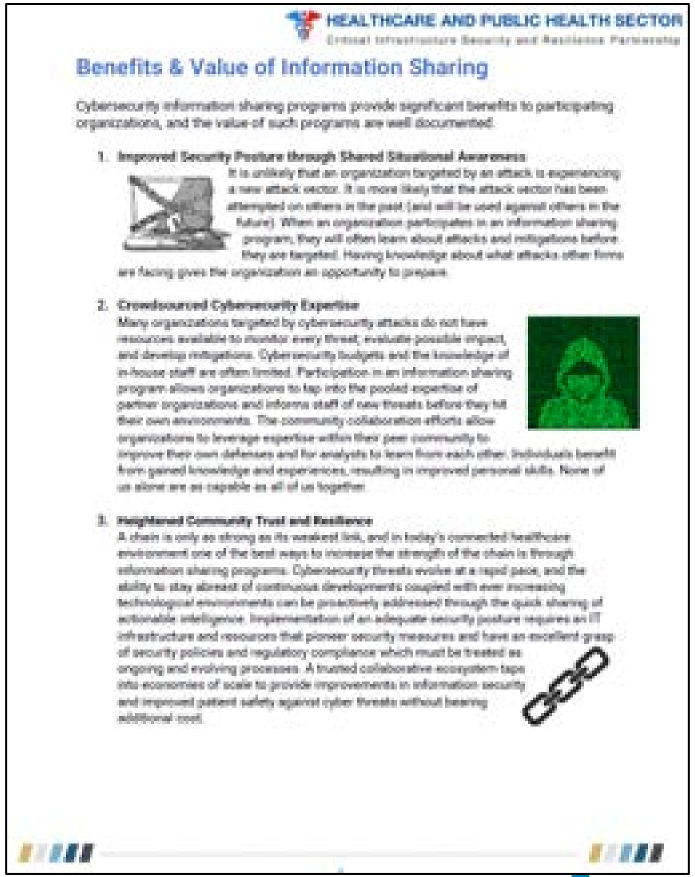
Information sharing programs, when done properly, produce significant benefit at low risk for the organizations that participate. This document was developed to provide Healthcare and Public Health Sector (HPH) organizations with a set of guidelines and best practices for efficient and effective information sharing. It addresses real and perceived barriers to information sharing that are often found from laws, regulations, corporate policies or management support, and will help organizations work through these obstacles.

We encourage HPH information sharing organizations to use this document as the basis of their own Information Sharing Best Practices Guideline. Organizations can customize the content provided here for their own information sharing environment.

HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership
HealthSectorCouncil.org

Benefits & Value of Information Sharing

- Improved Security Posture through Shared Situational Awareness
  - Similar to a “Neighborhood Watch” program
  - Early warning about attacks
  - Learn about effective defenses, controls and countermeasures
- Crowdsourced Cybersecurity Expertise
  - Community of knowledge and experience
  - Leverage experts
  - Learn from others
- Heightened Community Trust and Resilience
  - Risk management is an ongoing and evolving process
  - Rapid sharing of actionable intelligence
- Improved Cyber Security Innovation
  - Get involved with sector challenges, standards, and development of best practices



HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership

Benefits & Value of Information Sharing

Cybersecurity information sharing programs provide significant benefits to participating organizations, and the value of such programs are well documented.

1. **Improved Security Posture through Shared Situational Awareness**
   It is unlikely that an organization targeted by an attack is experiencing a new attack vector. It is more likely that the attack vector has been attempted on others in the past (and will be used against others in the future). When an organization participates in an information sharing program, they will often learn about attacks and mitigations before they are targeted. Having knowledge about what attacks other firms are facing gives the organization an opportunity to prepare.

2. **Crowdsourced Cybersecurity Expertise**
   Many organizations targeted by cybersecurity attacks do not have resources available to monitor every threat, evaluate possible impact, and develop mitigations. Cybersecurity budgets and the knowledge of in-house staff are often limited. Participation in an information sharing program allows organizations to tap into the pooled expertise of partner organizations and informs staff of new threats before they hit their own environments. The community collaboration efforts allow organizations to leverage expertise within their peer community to improve their own defenses and for analysts to learn from each other. Individuals benefit from gained knowledge and experiences, resulting in improved personal skills. None of us alone are as capable as all of us together.

3. **Heightened Community Trust and Resilience**
   A chain is only as strong as its weakest link, and in today's connected healthcare environment one of the best ways to increase the strength of the chain is through information sharing programs. Cybersecurity threats evolve at a rapid pace, and the ability to stay abreast of continuous developments coupled with ever increasing technological environments can be proactively addressed through the quick sharing of actionable intelligence. Implementation of an adequate security posture requires an IT infrastructure and resources that pioneer security measures and have an excellent grasp of security policies and regulatory compliance which must be treated as ongoing and evolving processes. A trusted collaborative ecosystem taps into economies of scale to provide improvements in information security and improved patient safety against cyber threats without bearing additional cost.

What Information to Share

Non-Technical

Technical

Strategic Intelligence

- Understand new and emerging threats
- Identify potential impacts from risks
- Help navigate through complex matters that come with these new risks

---

- Helps form corporate policy
- Influence IT and Infosec spending
- Adjust business plans

Operational Intelligence

- Threat actor tactics, techniques, and procedures (TTPs)
- Actionable information on specific weaponized attacks
- Shared Vulnerability and threat reports
- Situational awareness
- Effective responses / countermeasures

Technical Intelligence

- File hashes
- Command and control (C2) IP addresses
- Malicious URLs
- email headers (from address, subject)
- Most widely used and available form of intelligence
- Very time consuming and resource-intensive to use
- Easiest for adversary to change once their attack techniques are discovered

Automating the ingestion process, analysis, and sharing is imperative

- Efficient use of cyber security resources
- Volume of information
- Short-term duration for value of the information

What Information to Share (continued)

- Industry Best Practices
  - Peer sharing of current challenges, implementations and experiences
  - Corporate policies, procedures and governance
    - Get insight into how peers approach a problem
  - Share step-by-step procedures and templates (Crowdsourcing)
    - Get value faster than trying to do it alone
      - Share guidance on technical challenges
      - Step-by-step threat hunting

Recent best practice discussions

- Cyber security budgets
- CISO Organization Structure and Reporting Lines
- Addressing Third party Risk
- Presenting Cyber Risk to the Board
- Securing Internet of Things (IoT)
- Changes in Laws and regulations and the impacts to policies

Who To Share With

External Partners

- Public Entities / Government organizations
  - Law enforcement
    - Interpol
  - Regulators
- Private Entities
  - Industry associations
    - FIRST
    - HKCERT
    - GovCERT.HK
    - ISACA
  - Third-party service providers
  - Information sharing organizations such as Health-ISAC

Examples

[illegible] AND PUBLIC HEALTH SECTOR
[illegible] Security and Resilience Partnership

W[illegible]are With

[illegible] cybersecurity threats continue to increase and IT environments grow even more complex[illegible] need for an organization to implement measures for effective and efficient information sharing increases. One emerging challenge is addressing and managing risk from supply chain organizations and third-party providers. A recognition of shared responsibility across the HPH sector reduces the level of effort for one organization and allows for combined efforts to identify and mitigate supply chain risks that could impact many organizations.

The importance of community wide protections increases as additional IT services are off-loaded to third party providers. Organizations can significantly benefit from forward-looking practices, such as operational threat information combined with shared situational awareness, made available to them through information sharing programs.

Consider the following list of potential information sharing partners, and identify which partners fit best within your organization's information sharing strategy. You should establish an information sharing agreement with these organizations. In the case of the Health-ISAC, for example, a Membership Services Agreement outlines data sharing and classification requirements for the parties involved.

- External Partners
  - Public Entities - Law enforcement, regulatory bodies, public associations, government organizations such as the HHS Health Sector Cybersecurity Coordination Center (HC3)
  - Private Entities - Industry associations, third-party service providers, information sharing organizations such as Health-ISAC
- Internal Groups
  - Cyber Threat Intelligence Teams
  - Information Security Staff
  - Business Continuity and Disaster Recovery Professionals
  - Incident Response Teams
  - Education, Training & Awareness Teams

Internal Groups

- Cyber Threat Intelligence Teams
- Information Security Staff
- Business Continuity and Disaster Recovery Professionals
- Incident Response Teams
- Education, Training & Awareness Teams

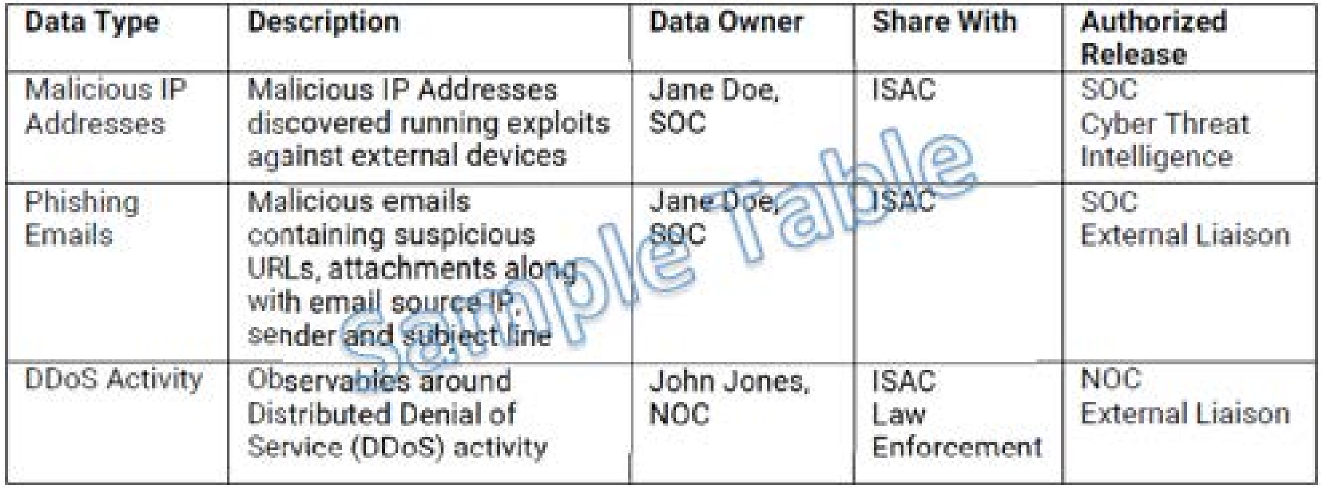
How to Share

- Legal Protections
  - Consider laws, rules and regulations
  - Many jurisdictions provide liability protection when sharing with peers and public sector
    - cyber threat indicators
    - defensive measures
- Partner with internal legal counsel
  - Explain value and scope information sharing
  - Engage your legal department early in the process
  - Consider running a healthcare-themed tabletop exercise with legal staff in attendance
  - Consider dedicating resources to legal outreach, as engaging and educating legal staff can be a long-term process

Internal counsel may be more willing to engage in finding solutions if they are included in the development of the program

How to Prepare for Information Sharing

- Establish Governance Models (Regulatory Compliance)
  - Identify data owners
  - Define each data type
    - Description
    - Internal data owner
    - Who can the data be shared with
    - Who is authorized to release the data
  - Create a Governance Body
    - Review processes and procedures
    - Review and catalogue findings from external entities
    - Raise awareness to internal security teams
    - Meet regularly (quarterly?) and review both internal and external findings



Data Type	Description	Data Owner	Share With	Authorized Release
Malicious IP Addresses	Malicious IP Addresses discovered running exploits against external devices	Jane Doe, SOC	ISAC	SOC Cyber Threat Intelligence
Phishing Emails	Malicious emails containing suspicious URLs, attachments along with email source IP, sender and subject line	Jane Doe, SOC	ISAC	SOC External Liaison
DDoS Activity	Observables around Distributed Denial of Service (DDoS) activity	John Jones, NOC	ISAC Law Enforcement	NOC External Liaison

Case Study #1

Phishing email from a compromised law firm with following IoCs:

Subject:	Urgent Information COVID-19 (Coronavirus) Update for your safety.
Displayed From:	broy@montielhodge[.]com
URL in body:	montielhodgefirm[.]com/ Redirects to O365 cred harvesting page in sandbox: hxxps://storage[.]googleapis[.]com/montielhodge/montielhodge[.]htm IP:160.153.71[.]128

Comments:

Made it past inbound email scanning service, but URL filter blocked it because it was less than 30 days old and uncategorized. Legit firm this was spoofing reported that they were hacked.

Case Study #2

Health-ISAC Members Observing Ongoing Social Engineering Attacks Targeting Service Desk and Call Centers

July 2022, Health-ISAC members report ongoing social engineering attacks targeting service desk and call centers to obtain confidential information from employees and initiate the theft of executive staff retirement accounts.

Threat actors obtained personally identifiable information (PII), likely from cybercriminals dark web forums, are leveraging improved social engineering tactics to bypass rudimentary security checks imposed by call center representatives. Some cases include the obfuscation of threat actor phone numbers via the use of Voice over IP (VoIP) providers and legitimate communication applications such as WhatsApp.

Due to the evolution of tactics, techniques, and procedures used in social engineering attacks, threat actors are likely to increasingly consider service desks and call centers as soft targets. It is recommended that Health-ISAC members review and harden call center policies to mitigate or counteract threat actors' continuous effort to discover ways to bypass identification processes in the furtherance of malicious activity.

Case Study #3

- Distributed Denial of Service Attack against an Industry Sector
- Example information sharing scenario from NIST Special Publication 800-150
    - A hacktivist group targets a select set of companies for a large-scale distributed denial of service (DDoS) attack. The group uses a distributed botnet that is loosely coordinated and controlled by members of the group. By analyzing traffic generated by the botnet, one of the companies targeted in the attack is able to determine that the actors are using a variant of a popular DDoS tool. The targeted companies are members of an ISAC and use the ISAC's discussion portal to establish a working group to coordinate incident response activities. The working group contacts the ISAC's law enforcement liaison, who coordinates with federal and international authorities to aid in the investigation and to gain court orders to shut down the actor's systems.
    - The working group contacts various internet service providers (ISPs), and provides information to aid in identifying abnormal traffic to their network addresses. The ISPs assist both the affected companies and law enforcement personnel by helping to identify the upstream and downstream traffic sources, implementing routing changes, and enforcing data rate limits on these sources. Using network traffic collected by the ISPs, law enforcement agencies can identify the command and control servers, seize these assets, and identify some members of the hacktivist group.
    - After a technical exchange meeting among the targeted companies, several companies decide to enlist the services of content distribution providers to deploy DDoS-resistant web architectures.

The Final Word – TRUST

- The success of information sharing in any community relies on the TRUST established between individuals.
- Trust is a requirement when an individual wants to share sensitive information with others.
- Trust is a human quality and cannot be replaced by automation.

- Get involved in your information sharing community
  - Help build and maintain trust networks
  - Host and attend in-person meetings
    - Conferences, Regional workshops, informal gatherings

- The personal relationships that you build with other professionals will help establish a network of trust in the wider information sharing community.

Thank You!

Errol Weiss, Health-ISAC
Chief Security Officer
+1 (321) 209-9898
eweiss@h-isac.org

Health-ISAC
www.h-isac.org

SHARING SINCE 2010
H-ISAC®
HEALTH - ISAC

Information Sharing Best Practices White Paper / Toolkit
https://h-isac.org/h-isac-information-sharing-best-practices/