Information Sharing Best Practices

TLP:WHITE This report may be shared without restriction. For Health-ISAC members—be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.

Abstract

Information-sharing programs produce significant benefits at minimal risk for the organizations that participate. This document provides Healthcare and Public Health Sector (HPH) organizations with a set of guidelines and best practices for efficient and effective information sharing strategies. It addresses barriers to information sharing often found in laws, regulations, corporate policies, or management support and will help organizations overcome these obstacles.

Contents

Purpose of this document 2

Benefits & Value of Information Sharing 3

What Information to Share 4

- Strategic Intelligence 4
- Tactical Intelligence 5
- Operational Intelligence 5
- Open-Source Intelligence (OSINT) 6
- Sharing of Industry Best Practices. 6
- Incident Response Information Sharing 7
- Threat Defender Content and Resources Sharing 7
- Media Response 7

How to Share 8

- Traffic Light Protocol 9
- Legal Protections 10

Who to Share With 11

How to Prepare for Information Sharing 12

Case Studies. 14

- Example 1: Untargeted Attack From Triage to Threat Indicator 14
- Example 3: Cyber Threat Indicators and Defensive Measures 15
- Example 4: Pro-Russian Hacktivists Launch Distributed Denial of Service Attack Against Healthcare Organizations1 15

The Final Word – TRUST 16

- Additional Reading 16

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

Purpose of this document

This document was developed in partnership between Health-ISAC and the Healthcare and Public Health Sector Coordinating Council (HSCC). Health-ISAC is a trusted community of critical infrastructure owners and operators within the global Healthcare and Public Health sector (HPH). The community is focused on sharing timely, actionable, relevant information on threats, incidents, vulnerabilities, best practices, mitigation strategies, and more. The HSCC is a coalition of private-sector critical healthcare infrastructure entities organized under US Presidential Policy Directive 21 and the National Infrastructure Protection Plan to partner with the government in identifying and mitigating strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Joint Cybersecurity Working Group (JCWG) is a standing working group of the HSCC, composed of almost 400 industry and government organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

The guidelines provide information about the following:

- What organizations need to do to prepare for information sharing
- What information to share
- How to share the data
- How to protect any sensitive information they receive
- Best practices to obtain necessary internal approvals, including legal approval for information sharing processes and identifying types of information that can be shared

This document operationalizes a 2019 publication by the HSCC — the Health Industry Cybersecurity Matrix for Information Sharing Organizations (HIC-MISO) — which provides an inventory of information sharing organizations and their key services for stakeholders wanting to know where and how to get started. When a health organization is new to information sharing, it can be confusing to navigate these sharing organizations and their services, and how to engage with them in a way that reduces risk for the organization.

Please visit https://healthsectorcouncil.org/ for more information about the HSCC and JCWG.

Benefits & Value of Information Sharing

Cybersecurity information-sharing programs provide significant benefits to participating organizations. There are many instances of increased security and risk mitigation because of these sharing initiatives.

1. Improved Security Posture through Shared Situational Awareness

It is unlikely that an organization targeted by an attack is experiencing a new attack vector. More likely still, the attack vector has been attempted on others in the past, and will be used against others in the future. Organizations that participate in an information-sharing program will often learn about novel attacks and mitigations before they are targeted—knowing what attacks other firms are facing allows the organization to prepare

2. Crowdsourced Cybersecurity Expertise

Many organizations targeted by cybersecurity attacks do not have the resources available to monitor every threat, evaluate possible impacts, 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. Community collaboration enables organizations to leverage expertise within the sector-specific security community to improve their defenses. These sharing communities also allow for analysts to learn from each other. Organizations benefit from current security strategies, and individuals benefit from gained knowledge and experiences, resulting in improved security posture on both an enterprise and individual level.

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 chain's strength is through information sharing. Cybersecurity threats evolve rapidly, and the ability to stay on top of continuous developments and with ever-increasing technological environments can be proactively addressed through the timely sharing of actionable intelligence. Implementing an adequate security posture requires an IT infrastructure with sufficient operational and security resources with members that have an excellent grasp of security policies and regulatory compliance. A trusted collaborative ecosystem taps into sizeable economies to provide improvements in information security for organizations and improved patient safety against cyber-threats without bearing additional costs.

4. Improved Cyber Security Innovation

Sector-wide awareness also significantly increases the avenues an organization has to receive advanced threat warnings. Cross-organization collaboration improves patient safety and supports the ability to establish reliable networks that help manage potential threats. As innovations in cyber-attacks continue to challenge the healthcare industry, security professionals will need to ensure their organizations are engaged and evolving along with unique sector challenges, standards, and best practices to keep patient care information safe.

What Information to Share

Threat intelligence is one of the most important data types to information-sharing programs. While some may believe that threat intelligence only includes information about malware, hacking techniques, and threat actors — threat intelligence data truly comes in a variety of forms and should encompass all risk vectors that could impact the healthcare industry, such as third-party risks, insider threats, cybersecurity risks, regulatory risks, and geopolitical risks. These are good examples of the types of threats that the healthcare industry faces daily, and therefore are prime areas to focus on when it comes to understanding the types of insights the information-sharing organization shares throughout the community. More recently, the scope of information sharing programs has also broadened to include sharing of threat detection and defense content such as SIEM rules, YARA rules, Response Playbooks, MITRE ATT&CK data, and analytics files to foster close collaboration between threat defense and detection teams.

Indeed, information sharing is successful only if the correct information is shared among its members and through information-sharing organizations built to protect critical infrastructure such as the Health Information Sharing and Analysis Center (Health-ISAC) and other specialized and government organizations identified in the HIC-MISO. This section highlights the types of information actively shared within the Health-ISAC community.

The following groupings of threat intelligence are routinely shared throughout the HPH industry and are disseminated through multiple channels offered by information-sharing organizations.

Strategic Intelligence

Strategic intelligence is the collection, processing, analysis, and dissemination of intelligence required to inform policy, help set and/or justify information security budgets, and refine business plans at the corporate and divisional levels. It typically focuses on new and emerging trends, changes in the cyber threat landscape, changes in laws and regulations, and the ever-evolving geopolitical and supply chain landscape.

Within the healthcare information-sharing community, strategic intelligence is created by intelligence analysts and the information-sharing community at large. Boards of directors can use strategic reports to define business priorities which are continually refined through the consumption of strategic intelligence production; a service offered by any of the information-sharing organizations in your enterprise that may participate. The broader stakeholder community, including cybersecurity researchers, law enforcement, government policymakers, and industry regulators, also influence strategic intelligence creation to produce the most effective and current threat-informed resilience strategies.

Members of the information-sharing community use strategic intelligence to proactively engage risk by using intelligence to identify emerging threats, thus minimizing potential adverse impacts on consumer organizations. Finally, strategic intelligence can help navigate the complex risk landscape and shed some light into unknown unknowns which may give client organizations an advantage in long-term business planning.

Here are a few examples of strategic intelligence shared within the information-sharing community:

- Analysis of the geopolitical landscape and its effects on the cyber landscape and the healthcare supply chain
- Guidance on privacy regulations such as General Data Protection Regulation
- Russia's Data Localization legislation
- Cyber Security Law of the People's Republic of China and impacts on the protection of intellectual property
- Risks of technologies used in specialized environments such as IoT/OT environments including medical devices and manufacturing facilities
- Risks of emerging technologies such as Artificial Intelligence; Machine Learning
- Guidance on new government cybersecurity strategies such as the National Cybersecurity Strategy of March 2023
- Insight on how to build business resilience in the face of the Russia/Ukraine war
- Analysis of adversarial nation state activity and the trends therein
- Illuminated risks of early adoption of new technology such as ChatGPT and other sophisticated artificial intelligence models
- Predictive analysis of emerging trends in cybercrime at all levels to create long term threat-informed defense strategies

All these examples could impact how an organization might change their risk posture, meet regulatory compliance, avoid policy violations, and preemptively mitigate developing security threats. Discussions about strategic intelligence issues help educate, prioritize, and cultivate proactive decision making within the HPH sector. For more information on strategic intelligence, please see the report, How Strategic Threat Intelligence Informs Better Security Decisions.

Tactical Intelligence

Tactical intelligence includes the details of threat actor tactics, techniques, and procedures (TTPs). Tactical intelligence provides information focused on the techniques that threat actors leverage to gain access to computerized systems and the mechanisms employed to carry out an attack, similar to what is highlighted in the MITRE ATT&CK Matrix.

Some examples of this type of intelligence are exploitation methods that threat actors use to carry out credential harvesting attacks (e.g., Credential Dumping, Brute Force), lateral movement (e.g., internal spear phishing, tainting shared content , and remote service exploitation), and command and control mechanisms (e.g., Domain Fronting, Fallback Channels, Domain Generation Algorithms).

Operational Intelligence

Operational intelligence is actionable information about specific weaponized attacks.

Operational intelligence is typically gathered by monitoring the internet, the dark web, and social media platforms to give intelligence consumers early notification of potential attacks on their industry or organizations.

Security researchers typically publish their research on new vulnerabilities and threats. These vulnerability and threat reports are shared amongst the community and provide members with situational awareness and mitigation strategies.

Open-Source Intelligence (OSINT)

Open-Source Intelligence (OSINT) is data collected from public sources, such as the internet, news sites, social media, and the dark web to be used in an intelligence context. OSINT is an essential part of the overall intelligence process as often these sources are the first to report about new threats and vulnerabilities. OSINT drives timeliness in intelligence production.

All these intelligence types serve important, specific purposes and complement each other to provide the health industry with both short and long-term insights and strategies to reduce risk.. Beyond threat intelligence, organizations can offer many different types of data, such as detection and defense recommendations, that should be shared throughout the information-sharing community.

Sharing of Industry Best Practices

Industry best practices are often shared among members of an information-sharing community. These practices continually evolve due to members requesting feedback from other organizations regarding implementing policies, procedures, and governance. The requests may address how organizations address a specific issue or risk and then share the information with the rest of the group. Direct feedback from peers helps members gain insight into how the industry approaches a problem or challenge and can inform the member's decision-making process and strategy, and lead to the refinement of such processes. Understanding the challenges and successes that peers have experienced is invaluable information. Some examples in this area are:

1. Addressing Third-Party Risk
2. Intelligence Gathering Techniques
3. Presenting Cyber Risk to the Board
4. Securing the Internet of Things (IoT)
5. Securing Big Data
6. Changes in Laws and Regulations and the Impacts to your Policies

Best practices typically reference standards and frameworks designed to be used across industries. Often, there are areas of ambiguity in these standards that organizations can help clarify by sharing key insights with the community members. In addition to gaining clarity, understanding how other members use these standards provides a great deal of insight into methods of effective implementation.

Sharing step-by-step procedures or templates enable members of an information-sharing organization to become productive faster, protect their network better and become more resilient than trying to do it alone. Sharing guidance on technical challenges is also commonplace within an information-sharing organization. Typical topics within these forums include how to quarantine/eradicate specific malware, tool guidance (including command-line tools), or extensive guidance on hunting for threats within your environment. These types of knowledge sharing often occur in real-time across the membership of an information-sharing organization.

This is especially useful in times of an emerging cyber threat that escalates to an elevated status. Whether discussing best practices or providing general guidance, this information is shared in various forums such as regularly scheduled webinars, workshops, summits, and focused discussions.

It is important to note that members of an information-sharing organization benefit by turning these activities into actionable communications that a non-technical audience can leverage through standardized templates and sample communications. These assist members in communicating effectively to their leadership and stakeholders. These types of communications serve multiple purposes, such as ensuring a clear and consistent message across the health industry.

Incident Response Information Sharing

The health industry is heavily regulated and is subject to specific breach reporting requirements. In cyber crises, information flows must be clear, consistent, and accurate. Information-sharing organizations are positioned to provide that clarity during these times.

Whether a crisis affects the entire industry or a single entity, information-sharing organizations share pertinent information across the industry while keeping the victim's identity protected. In an industry that is negatively impacted by misinformation, information-sharing organizations provide clarifying details of an event, correct public misinformation, and provide clarity in a time of ambiguity. The rapid sharing of situational awareness is made possible because information-sharing organizations offer a medium for directly from the impacted organizations to share their experiences.

Threat Defender Content and Resources Sharing

Until now, information sharing programs have had their scope largely limited to the sharing of threat indicators of compromise (IOCs) and attacker tactics, techniques, and procedures (TTPs). While sharing IOCs and TTPs is critical to proactively mitigate attacks, modern cyber security programs are expanding the scope of information sharing by including threat defender and defense content and resources. Such resources include sharing SIEM rules, YARA rules, MITRE ATT&CK data, and Automated Response Playbooks, and more.

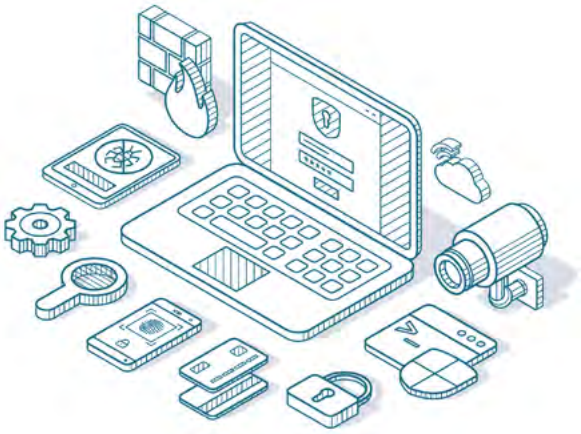
Organizations can benefit from sharing such defense and detection resources as they foster close collaboration between the threat defenders across the larger community of information security professionals and enables doubling down of efforts against attackers by sharing proven operational knowledge around effectively mitigating attacks. An organization defending itself from an attack can benefit from the knowledge shared by other organizations such as what SIEM rule should be written to proactively detect a specific attack or what YARA rule should be deployed on an endpoint detection and response system (EDR) or an intrusion prevention/detection system (IDS/IPS) to identify and detect a certain malware.

Media Response

Information-sharing organizations can share responses to media inquiries as a representation of the health industry, rather than as an individual member. For example, the media may inquire about the impact of new privacy regulations on the HPH industry. Rather than hearing from one individual company, information-sharing organizations can poll their members and pull together a collective response that is a better representation of the entire industry. Health-ISAC can facilitate anonymous feedback, provide a more holistic representation of the health industry, and drive a clear and consistent message. A community response can include sharing talking points with its members to aid in media inquiries, especially during an incident. These talking points can provide guidance as to what is appropriate to share with the media.

How to Share

Sharing guidelines are intended to control the publication and distribution of threat information. They also exist to help prevent the dissemination of information that, if improperly disclosed, may have adverse consequences for an organization, its customers, or business partners. Information-sharing rules should consider the recipient's trustworthiness, the sensitivity of the shared information, and the potential impact of sharing or withholding specific types of information. Types of information sharing include:



Firm-Derived Information:

- Do not share sensitive information about specific impacts or details that could be used to identify the firm
- Safeguard Personally Identifiable Information (PII), Protected Health Information (PHI), or proprietary information
- If guidance is not clear, request permission to share data that is not your own

Sharing Third Party and Vendor derived information:

- Share in accordance with third-party and vendor disclosure agreements
- Do not violate confidentiality agreements

Share quality information

- Include confidence levels in any analyst judgments made in your reporting
- Share source information as permitted (do not source specific vendors by name; instead, say "security/ intelligence vendor;" do directly source Open-Source Information)
- Share analysis and include the "so what" to explain why this information is essential to you and your peers

Sanitize and Redact Security Reports:

- Do share analysis
- Do not share the impact or consequences to the firm
- Do share open-source information
- Do not share vendor names
- Do not share author information
- Do share approved IOCs

For more sophisticated organizations or those that have the resources to invest in automation, the following tips can be used to Automate Intelligence Approval, Processing, Sharing, and Actioning Processes

- Orchestrate threat data flow from detection technologies and reporting tools to threat intelligence platforms (TIP) for review and approval
- Leverage TIP orchestration to automatically review and approve the information to be shared. Predefine rules to classify which and what type of information can be shared externally
- Process information shared by other partners using automated TIPs to gather more context and relevance

- Correlate received information, through TIPs, with internal threat intelligence and telemetry to enrich, add context, and score intelligence
- Automatically share back processed threat intelligence with more context and confidence with information sharing partners
- Automate actioning of threat data in response technologies using TIPs
- Avoid manual processes for processing and sharing threat intelligence to scale threat intelligence operations, derive more value from information sharing programs and reduce analyst burden

Traffic Light Protocol

The Traffic Light Protocol (TLP) is used by information-sharing organizations, such as Health-ISAC, to set strict information handling guidelines and procedures for the recipients. All information submitted, processed, stored, archived, or disposed of, is classified, and handled in accordance with the following:

- Unless otherwise specified, all information is treated as confidential information (TLP:AMBER) and is not disclosed to parties outside of the information-sharing organization without the permission of the originator
- Information classified as TLP:GREEN, TLP:AMBER, or TLP:RED must be disclosed, transported, stored, transmitted, and disposed of, safely and securely using controls appropriate to the classification level. These controls include but are not limited to, encryption, shredding, securely erasing and degaussing of media

The table below describes the Health-ISAC classifications of information and intended audiences. Organizations can create their own TLP definitions, and therefore, there are many nuances that exist. We urge the reader to be familiar with the TLP definitions of their respective information sharing community.

Traffic Light Protocol

Classification	When Should It Be Used?	How May It Be Shared?
TLP:RED	Sources may use **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Restricted to a defined group (e.g., only those present in a meeting or recipient of a defined group.) Information labeled **TLP RED** should not be shared with anyone outside of the group
TLP:AMBER	Sources may use **TLP:AMBER** when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	This information may be shared with Health-ISAC members and Health-ISAC member employees with a need to know. Generally, alerts with the Health-ISAC **TLP AMBER** classification will be kept behind the Health-ISAC secure portal.
TLP:GREEN	Sources may use **TLP:GREEN** when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Information within the **TLP GREEN** category may be shared with Health-ISAC members and trusted partners (e.g., CERTS, law enforcement, government agencies and other ISACs). Information in this category is not to be shared in public forums or over public channels.
TLP:WHITE	Sources may use **TLP:WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	**TLP WHITE** information may be shared freely subject to standard copyright rules.

Source: Health-ISAC Traffic Light Protocol (TLP) Definition

Legal Protections

Cybersecurity Information Sharing Act of 2015 (CISA2015)

The Cybersecurity Information Sharing Act of 2015 (CISA2015) – was signed into law on December 18, 2015, and provides private sector entities with liability protection when sharing information with peer firms and public sector government organizations.

Section 104(c) of CISA2015 states that private sector organizations may, notwithstanding any other law, share cyber threat indicators or defensive measures with peer firms, ISACs and ISAOs. **CISA2015 protects any private entity from liability arising from sharing a cyber threat indicator or defensive measure.**

More details, examples and guidance is available in this document, *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015*, published by The Department of Homeland Security and The Depart of Justice in October 2020, and available here.

The Freedom of Information Act (FOIA)

The Freedom of Information Act (FOIA) is a US law that allows the public to request access to records from any US federal agency. FOIA does not apply to private sector organizations, including Health-ISAC, meaning a FOIA cannot be issued to Health-ISAC requesting the release of sensitive member information.

Information Sharing and GDPR

The European Union General Data Protection Regulation, or"GDPR," went into effect in2018 and provides individuals in the European Union (EU) and the European Economic Area (EEA) rights and control over their personal information.

GDPR Article 6(1)(f) states that processing personal data is lawful when it "is necessary for the purpose of the legitimate interests pursued by the controller or by a third party." The processing of personal data under this Article must meet a three-step test: legitimacy, necessity, and a balancing of interests. A 2018 paper, Threat Information Sharing and GDPR: A Lawful Activity that Protects Personal Data, outlines how the processing of personal data in threat information by an ISAC and its Members meets this criteria. Specifically,

- The ISAC's and its Members' interests – sharing information to prevent fraud and improve network security against cyberattacks – are legitimate uses of personal data under GDPR.
- The processing of personal data for these interests is necessary and proportionate as a critical component of ensuring network and system security and the prevention of fraud.
- Providing that appropriate privacy safeguards are adopted by the ISAC and its Members, the interests are balanced because controls are implemented to ensure that the goal of preventing or stopping fraud and ensuring the security of members' networks are not outweighed by the interests of the data subjects whose personal data is processed. The interests of data subjects are aligned with those of the ISAC and Members.

Who to Share With

As cybersecurity threats continue to increase and IT environments grow even more complex, the need for an organization to implement measures for effective and efficient information sharing increases. One emerging challenge is addressing and managing risk from upstream organizations and third-party providers. Recognizing shared responsibility across the HPH sector allows for combined efforts to identify and mitigate supply chain risks that could impact many organizations.

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

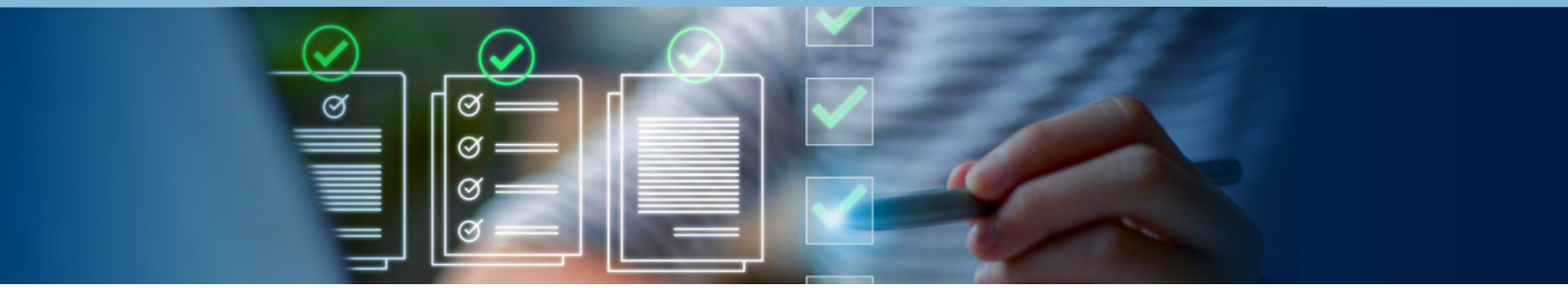
Consider the following list of potential information-sharing partners, and identify which partners fit best within your organization's information-sharing strategy. You should establish an information-sharing agreement with these organizations. In the case of the Health-ISAC, for example, a Membership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

External Partners

- Public Entities - Law enforcement, regulatory bodies, public associations, and 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
- Fusion Centers
- Information Security Staff
- Physical Security Staff
- Business Continuity and Disaster Recovery Professionals
- Incident Response Teams
- Education, Training & Awareness Teams
- Legal Teams
- Senior Leadership



How to Prepare for Information Sharing

The following recommendations will guide you through the initial preparation to perform before you join an Information Sharing program.

1. Establish Your Information Sharing Goals & Objectives. It is crucial to start by establishing the overall purpose of your information-sharing program, especially in the business context of your environment. The strategy should outline its scope, identify which information-sharing organizations you will partner with, and detail the roles and responsibilities of your internal teams.

2. Establish Governance Models To Ensure Compliance. Identify data owners across the organization that could be candidates for information sharing participants, such as your internal Security Operations Center (SOC), malware research team, digital forensics unit, incident response team, threat management team, or cyber threat intelligence team.

Categorize your Information-Sharing Assets Develop a table that lists each data type, its description, the corresponding internal data owner, which external organizations the data can be shared with (ISACs, ISAOs, Law Enforcement, etc.), and who is authorized to release the data (see example below).

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 E-mails	Malicious e-mails containing suspicious URLs, attachments along with e-mail 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

3. Create a Governance Body. Assemble a steering committee, working group, or informal body to review these processes and procedures to establish a consensus around the governance of sharing information externally from the organization. The same governance body can also review and catalogue findings from other external entities to enhance knowledge and bring awareness to internal security teams. The governance body should meet regularly (at least once a quarter) and review both internal and external findings.

4. Embrace Third Party Review. Consider voluntarily gaining accreditation or look for others who have embraced the performance of an audit. This may be proven in many different types of forums, including but not limited to financial reports, Privacy, Security and Cybersecurity Audits, Accreditation and Certification. When organizations handling data voluntarily go through audits/certification processes, they show trading partners they have been vetted and can be trusted. When accepting another's accreditation/certification credentials, first be sure to confirm that the scope of the audit includes the data regarding the information your organization will be sharing.

5. Establish Sanitization Rules. Organizations should establish a process to ensure no proprietary or sensitive information is disclosed when sharing information with external entities. Refer to the HIPAA Minimum Necessary rule when deciding which sensitive information, such as PHI or PII, should be disclosed. To completely redact PHI or PII, it is recommended to use the "safe harbor method" listed in the HIPAA De-Identification document. Offering a limited data set may be the preferred method if certain information is necessary for shared information to be meaningful.

6. Bring the Legal Department into the Information Sharing Process. Internal legal counsel may not fully appreciate the value or scope of information sharing and often see only the risks. Organizations experience roadblocks to information-sharing activity because legal counsel within their organization has no experience with the information-sharing process thus not recognizing the value information-sharing programs can provide and see the overall program as adding more risk to the firm. Educating legal experts is an essential step towards information-sharing.

7. Engage the Legal Department Early in the Process of Establishing an Information-Sharing Program. Consider running a healthcare-themed tabletop exercise with legal staff in attendance so they can better understand the problems that HPH IT and Information Security professionals face. Internal counsel may be more willing to engage in finding solutions if they are included in the development of the program.

8. Consider Dedicating Resources to Legal Outreach. Engaging and educating legal staff can be a long-term process. Engaging the legal department can provide concrete benefits to the speed and flexibility with which the HPH sector can act during widespread security incidents such as WannaCry. A primary concern during these types of events is the timeliness and accuracy of the information being shared. Reducing legal roadblocks allows more HPH organizations to feel comfortable discussing and actively sharing and providing more detailed data for the technical community to analyze and implement ways to better protect their own firm.

Case Studies

The following case studies offer examples of information sharing in different circumstances. Every situation is different, and these examples can be adapted to suit your organization's unique information-sharing requirements.

The first example only includes four pieces of data, but the data is highly valuable because an adversary's infrastructure may only be active for a few hours or days. Therefore, information shared during an active attack can be useful only if the infrastructure is still operational.

Example 1: Untargeted Attack From Triage to Threat Indicator

Organization A receives thousands of malicious untargeted e-mail messages per day. 70% of them are rejected thanks to email filters. 20% are inspected for malicious content in quarantine and rejected. 10% evade all automated filters and are delivered to an end user's desktop. These trigger a response from Security Operations and a new collection of "fresh" indicators to be shared. Below is an example of the indicators shared with the Health-ISAC membership by Organization A.

IOCs related to a phishing email sent to an executive director at the company.

Confidence Level
High

Threat Indicators
Subjectline -
RES: Firewall document to be approved on Friday - see details for Legal [PNA-JUR_SP.FID689684]

Attachment name -
Firewall Implementation Strategy for Vaccine Localization TT 17May23 (Review PNA_May 17 2023) (48702373.1).docx

Sender address -
naun@pn.com.br

URLs/Domains -
http[:]//links[.]em[.]bevmo[.]com
http[:]//links[.]em[.]bevmo[.]com/ctt?m=27771848&r=NzAyMjg2Njc1OTk1S0&b=0&j=MjM4MTEzMjk1NAS2&k=productImg4&kx=1&kt=12&kd=https%3A%2F%2Fshoremenoutfittershunting.com%2Fnew%2Fauth%2Flurrdn%2F%2F%2F%2Fc2FicmluYS5yZXN0cmVwb0BtZXJjay5jb20=

https[:]//shoremenoutfittershunting[.]com
https[:]//shoremenoutfittershunting[.]com/new/auth/lurrdn/c2ficmluys5yzxn0cmvwb0btzxjjay5jb20

https[:]//yjsjyktaif64218291090f9[.]lojai[.]ru
https[:]//yjsjyktaif64218291090f9[.]lojai[.]ru/Mc2ficmluys5yzxn0cmvwb0btzxjjay5jb20

Analyst Notes
The link redirect 2 times for a total of 3 different URLs/domains till reaching the third and final destination.

Example 2: Targeted Campaign

The second example provides insight into the other end of the information-sharing spectrum. An in-depth analysis of a specific, targeted campaign adds value by illustrating attacker detailed activity and is especially useful for analysis and strategic decision-making.

Organization B becomes aware of a potentially targeted spear phishing campaign through a trusted third party. They observe and record activity based on this information. After a few days, no new indicators are received and the campaign ends.

Organization B develops and shares a full report to the Health-ISAC, exposing the details of the campaign and relevant indicators:

- **Summary:** provides context to the event as applicable
- **Analysis:** Outlines harvested indicators from the campaign, noting details of the timing and similarity of malicious content relative to the organization the attack attempted to impersonate, including details of the infrastructure used to launch the attack.
- **High-Level Tactics, Techniques and Procedures:** Highlights vital elements of attacker tradecraft and approach to this specific campaign.
- **Mitigations, Recommendations, Indicators of Compromise:** Detailed steps taken to block and detect inbound attacks or outbound communications if a recipient is impacted.

Example 3: Cyber Threat Indicators and Defensive Measures

In a June 2016 posting on Sharing Guidance, DHS provided examples of cyber threat indicators and defensive measures. The items below are good examples of indicators and analysis that your organization could provide to the information-sharing community:

- Malware
- Information Regarding the Intrusion Vector and Method of Establishing Persistent Presence
- Information Regarding When Unauthorized Access Occurred
- Information Regarding How the Actor Moved Laterally Within a Network and How Network Protections Were Bypassed
- Information Regarding the Type of Servers, Directories, and Files That Were Accessed
- Information Regarding What Was Exfiltrated and the Method of Exfiltration
- Information Regarding the Damage or Loss Caused by the Incident, Including Remediation Costs

Example 4: Pro-Russian Hacktivists Launch Distributed Denial of Service Attack Against Healthcare Organizations1

The following is a synopsis of a mass healthcare-targeting event being remediated by knowledge obtained through information sharing.

On January 27, 2023, Organization A observed Killnet associate, KillMilk, releasing a Distributed Denial of Service (DDoS) targeting list on Telegram. Telegram is an encrypted messaging platform. The targeting list announced on January 27 was unique because it exclusively targeted healthcare. The day after, January 28, a twitter user posted the targeting list, making it public. The list was shared with a healthcare sector information sharing organization that discovered the list contained numerous organizations from the Health-ISAC community. DDoS attacks began taking place on the day the adversary specified, [January 30], but were successfully mitigated through rapid sharing of IOCs pertaining to Killnet infrastructure, targeted alerts sent from the information sharing community to organizations present on the list and sharing best practices with the sector at large.

Organizations that were members of the information sharing organization not only possessed the advantage of increased visibility into the cyber threat landscape, but also were able to incorporate a set of crowdsourced industry-specific best practices.

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.

We encourage you to get involved in your applicable industry-specific information-sharing community to help build and maintain networks of trust. Host and attend in-person meetings whether at a conference, regional workshop, or informal gathering of security professionals in your city. The personal relationships that are built with other professionals will help establish a network of trust in the wider information-sharing community and help maximize the benefits received from membership.

Additional Reading

The National Institute of Standards and Technologies (NIST) published a thorough document providing additional guidance and factors to consider beyond what was covered in this document. For additional reading, we recommend the NIST Guide to Cyber Threat Information Sharing, NIST Special Publication 800-150, October 2016.

Feedback and suggestions on this document are encouraged and welcome.
Please e-mail **contact@h-isac.org**