Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

HEALTH INDUSTRY CYBERSECURITY INFORMATION SHARING BEST PRACTICES

MARCH 2020

HEALTH INDUSTRY CYBERSECURITY

INFORMATION SHARING BEST PRACTICES

March 2020

Information sharing programs, when done properly, produce significant benefit at low 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. 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.

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

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.

If your organization would like to use any or all of this document as your own branded reference for your enterprise or association/professional society membership, please contact Greg.Garcia@HealthSectorCouncil.org to request an editable Word version.

Contents

Purpose of this document **1**
Benefits & Value of Information Sharing 2
What Information to Share 3
Strategic Intelligence 3
Tactical Intelligence 4
Operational Intelligence 5
Technical Intelligence 5
Open Source Intelligence (OSINT) 5
Sharing of Industry Best Practices 5
Incident Response Information Sharing 6
Media Response 7
How to Share **7**
Traffic Light Protocol 8
Legal Protections 10
Who to Share With 10
How to Prepare for Information Sharing 11
Case Studies 13
Example 1: Untargeted attack from triage to threat indicator **14**
Example 2: Targeted campaign 14
Example 3: Cyber threat indicators and defensive measures 15
Example 4: Distributed denial of service attack against an industry sector[1] 15
Conclusion **16**
The Final Word – TRUST 16

Information Sharing Best Practices

Purpose of this document

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 interested in information sharing 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. The guidelines provide information about:

1. What organizations need to do to prepare for information sharing, what information to share, how to share the information, and how to protect any sensitive information they receive; and,
2. 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 was developed by the Healthcare and Public Health Sector Coordinating Council (HSCC) – a coalition of private-sector critical healthcare infrastructure entities organized under Presidential Policy Directive 21 and the National Infrastructure Protection Plan to partner with government in the identification and mitigation of 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 more than 250 industry and government organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

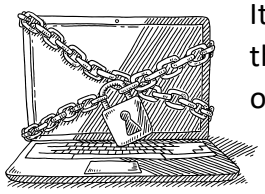
This document operationalizes a 2019 publication by the HSCC – the Health Industry Cybersecurity Matrix for Information Sharing Organizations (HIC-MISO) - which provides an inventory of information sharing organizations and their key services for stakeholders wanting to know where and how to get started. 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, and the value of such programs are well documented.

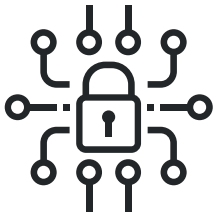
1. **Improved Security Posture through Shared Situational Awareness**
   It is unlikely that an organization targeted by an attack is experiencing a new attack vector. It is more likely that the attack vector has been attempted on others in the past (and will be used against others in the future). When 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 is 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.

4. **Improved Cyber Security Innovation**



Sector-wide awareness also significantly increases an organization's ability to develop advanced threat warnings. Cross-organization collaboration improves patient safety and supports the ability to develop trustworthy networks that help manage potential threats. As innovations in cyber attacks continue to challenge the healthcare spectrum, security professionals will need to ensure their organizations are engaged and evolving along with sector challenges, standards, and best practices in order to sustain patient care information.

What Information to Share

Threat intelligence is one of the primary data types important 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 cyber risks that could impact the health 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 health industry faces daily and are prime areas to focus on when it comes to understanding the types of information that the information sharing organization shares throughout the community.

Indeed, information sharing is successful only if the right information is shared among its members and through critical infrastructure information sharing organizations like the Health Information Sharing and Analysis Center and other specialized and government organizations identified in the HIC-MISO. This section highlights the types of information that are being actively shared within the Health ISAC and throughout the information sharing community.

The following groupings of threat intelligence are routinely shared throughout the HPH industry, leveraging multiple channels offered by information sharing organizations.

Strategic Intelligence

Strategic intelligence pertains to the collection, processing, analysis, and dissemination of intelligence that is required to form 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 landscape.

Within the health care information sharing community, strategic intelligence is created by numerous analysts and the information sharing community. Strategic reports can be used by boards of directors to set business priorities and be further refined through services offered by any of the information sharing organizations your enterprise may participate. Strategic Intelligence is also influenced by the broader stakeholder community including cybersecurity researchers, law enforcement, government policy makers, and industry regulators.

Members of the information sharing community use strategic intelligence to proactively understand new and emerging threats, identify the potential impacts that risks can have on their organization, and help navigate the complex matters that come with these new risks.

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

- Analysis of the geopolitical landscape and the effects on the cyber landscape
- 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.

All these examples could impact how an organization might monitor for intrusions, regulatory compliance, and policy violations. Discussions about strategic intelligence issues help educate, prioritize, and drive action within the HPH sector.

Tactical Intelligence

Tactical intelligence includes the details of threat actor tactics, techniques, and procedures (TTPs). Tactical intelligence provides information focused on the techniques that are leveraged by threat actors to gain access into computerized systems and the mechanisms employed to carry out an attack, similar to what is highlighted in the MITRE ATT&CK Matrix[(2)].

Some examples of this type of intelligence are procedures that threat actors use to carry out credential harvesting attacks (e.g. Credential Dumping, Brute Force), lateral movement (e.g. Pass-the-hash, pass-the-ticket, 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 sites to give organizations earlier notification of potential attacks to their industry or organizations. Security researchers typically publish their research on new vulnerabilities and threats. The vulnerability and threat reports are shared amongst the community and provides the members with situational awareness on these new threats as well as how to respond.

Technical Intelligence

Technical intelligence threat indicators include items like file hashes, command and control IP addresses, malicious URLs, and email headers. Technical intelligence is the most widely used and available within the cybersecurity industry. It can also be the most time consuming and resource-intensive type of intelligence to use. On the other hand, it is also the easiest for an adversary to change once their attack techniques are discovered. Automating the ingestion process, analysis, and sharing of this intelligence is important for several reasons, including efficient use of scarce cyber security experts, the volume of information available and the short-term value of the information when used to protect enterprise networks.

Open Source Intelligence (OSINT)

Open Source Intelligence (OSINT) is data collected from public sources, such as the internet and news media sites, to be used in an intelligence context. OSINT is an important part of an overall intelligence program as often these sources are the first to learn and report about new threats and vulnerabilities.

All these intelligence types serve important, specific purposes and, if done correctly, complement each other to provide the health industry with its short- and long-term risk reduction initiatives. However, beyond threat intelligence, organizations can offer many other types of data 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. Community members request feedback from other organizations regarding implementation of policies, procedures and governance. The requests may address how organizations are addressing a certain issue or risk and then share the information to the rest of the group. Hearing directly from peers helps members gain insight into how the industry is approaching a problem or challenge and can inform the member's decision-making process and strategy. Understanding the challenges and successes that your 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 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 that are designed to be used across industries. Often, there are areas of ambiguity in these standards that an organization can help clarify by sharing key insights with the community members. In addition to gaining clarity, understanding how other members are using these standards provides a great deal of insight in effectively implementing those standards within their own organizations.

Sharing of step-by-step procedures, or templates, enables members of an information sharing organization to realize value faster than trying to do it alone. Sharing guidance on technical challenges is also common practice within an information sharing organization. Common topics within these forums include how to quarantine/eradicate specific malware, tool guidance (including command-line), or step-by-step guidance on hunting for threats within your environment. These types of knowledge sharing often occur in real time across the information sharing organization membership.

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 on a topic, information sharing organizations share this type of information in a variety of forums such as their 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 can be leveraged by a non-technical audience in the form of standardized templates and sample communications. These sample communications assist members in communicating effectively to their leadership and their 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 accordingly is subject to specific breach reporting requirements. In the event of a cyber crisis, it is imperative that information flows are 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 can share pertinent information across the industry while keeping the victim's identity protected. In an industry that can be negatively impacted by misinformation, information sharing organizations can provide clarifying details of an event, correct any misinformation that is public, and can provide clarity in a time of ambiguity. The rapid sharing of

accurate situational awareness is made possible because information sharing organizations provide a mechanism to share this information directly from the impacted organization.

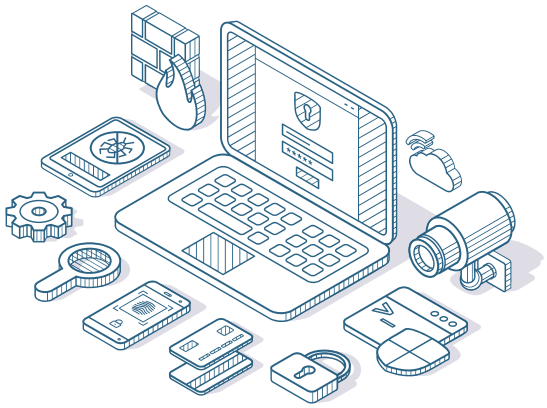
Media Response

Information sharing organizations can share responses to media inquiries as a representation of the health Industry as a whole, rather than 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 its members and pull together a collective response that is a better representation of the industry. The ISAC can facilitate anonymous feedback, provide a more holistic representation of the health industry, and drive a clear and consistent message. The 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 to the media.

References:

1) Recorded Future, "How Strategic Threat Intelligence Informs Better Security Decisions", Sept 13, 2018, https://www.recordedfuture.com/strategic-threat-intelligence/
2) Mitre ATT&CK: https://attack.mitre.org/

How to Share



Sharing guidelines are intended to control the publication and distribution of threat information, and help to prevent the dissemination of information that, if improperly disclosed, may have adverse consequences for an organization, its customers, or its business partners. Information sharing rules should take into consideration the trustworthiness of the recipient, the sensitivity of the shared information, and the potential impact of sharing (or not sharing) specific types of information.

- 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), sensitive or confidential 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 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; rather, say "security/intelligence vendor". Do directly source Open Source Information).
  - Share analysis and include the "so what" to explain why this information is important to you and your peers.
- Sanitize and Redact Security Reports:
  - Do share analysis
  - Do not share 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.

Traffic Light Protocol

The Traffic Light Protocol (TLP) is used by information sharing organizations, such as the 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 classification:

- Unless otherwise specified, all information is treated as confidential information (Amber) and is not disclosed to parties outside of the information sharing organization without the permission of the originator.
- Information classified as Green, Amber, or Red must be disclosed, transported, stored, transmitted and disposed of, in a safe and secure manner using controls appropriate to the level of classification. These controls include, but are not limited to, encryption, shredding, securely erasing and degaussing of media.

The table below describes the classifications of information and intended audiences.

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.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
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.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
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.	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.
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.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Source: US-CERT, Traffic Light Protocol (TLP) Definitions and Usage https://www.us-cert.gov/tlp

Legal Protections

Cybersecurity Information Sharing Act of 2015 (CISA)

The Cybersecurity Information Sharing Act of 2015 (CISA) – 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 CISA states that private sector organizations may, notwithstanding any other law, share cyber threat indicators or defensive measures with peer firms, ISACs and ISAOs. CISA protects any private entity from liability arising from sharing a cyber threat indicator or defensive measure.

What about the Freedom of Information Act (FOIA)?

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

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 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

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's important 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 roles and responsibilities for your internal teams.

2. **Establish Governance Models (Regulatory Compliance)**
   Identify data owners across the organization that could be candidates for information sharing, 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.

3. **Categorize your information sharing assets.** Develop a table that lists each data type, a description of the data type, the 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 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

Sample Table

4. **Create a governance body.** Assemble a steering committee, working group, or informal body to review these processes and procedures and to establish consensus around the governance of sharing information externally from the firm. 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.

5. **Embrace Third Party Review**. Consider voluntarily gaining accreditation / certification and/or look for others who have embraced the performance of a business/operation/privacy/security/cybersecurity audit. This may be proven in many different types of forums such as, but not limited to business/financial reports, Privacy, Security and Cybersecurity Audits, Accreditation and Certification. When organizations handling data voluntarily go through audits/certification processes they show their trading partners they have been "vetted" and are able to be trusted. When accepting another's accreditation / certification credentials, first be sure to confirm that the scope of the audit includes the data for which your organization will be sharing.

6. **Establish Sanitization Rules**
   Organizations should establish a process to ensure no proprietary or sensitive information is disclosed when information is released for sharing. Refer to the HIPAA Minimum Necessary rule when deciding which sensitive information, such as PHI or PII, should be disclosed. Complete redaction of the PHI or PII, refer to HIPAA De-Identification, the "safe harbor method", may be appropriate. Offering a limited data set may be the preferred method if certain information is necessary for shared information to be meaningful.

7. **Bring the Legal Department into the Information Sharing Process**
   Keep in mind that your internal legal counsel might not fully understand the value and scope information sharing. Organizations often experience roadblocks to information sharing activity because the legal counsel within their organization have no experience with information sharing processes, do not recognize the value information sharing programs can provide and see the overall program as adding more risk to the firm. Educating legal experts is an important step in engaging with the information sharing process.

8. **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 professionals face. Internal counsel may be more willing to engage in finding solutions if they are included in the development of the program.

9. **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 incidents such as WannaCry. The primary concern during these types of events is the timeliness and accuracy of information being shared. Reducing legal roadblocks allows more HPH organizations to feel comfortable discussing and actively sharing, as well as providing more detailed data for the technical community to analyze and ultimately implement ways to better protect their own firm.

Case Studies

The following case studies offer examples of information sharing in different situations and at different levels of detail. Every situation is different, and these examples can and should 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. Information that is shared during an active attack can be of value only if the infrastructure is still active.

Example 1: Untargeted attack from triage to threat indicator

Organization A receives thousands of malicious untargeted e-mail messages per day. 70% are rejected thanks to domain-name authentication or blocked by reputation. 20% are inspected for malicious content in quarantine and rejected. Unfortunately, 10% evade all automated filters and are delivered to an end user's desktop. These trigger a response from Security Operations, and the collection of "fresh" indicators to be shared. Below is an example of the indicators shared to the H-ISAC membership by Organization A:
The second example provides insight to the other end of the information sharing spectrum. In-

Hello All,

Please be advised of the following IOCs that lead to a fraudulent OneDrive sign in page.

Suspect Subject: [EXTERNAL] Document- Proposal PO
Suspect Sender: nward[@]micromerchantsystems[.]com
Suspect Phishing Link: hxxps://kellersproauto-my[.]sharepoint[.]com/:o:/g/personal/nate_kellersproauto_com1/Ei30sLrLwlNDrsDxacmNh-rBHfi_hxDKJ8QgBXRErmiH8A?e=8t9Pkk
Suspect Landing Page: hxxps://www[.]surveygizmo[.]com/s3/5247299/

Thanks,

depth analysis of a specific, targeted campaign adds value by illustrating attacker activity in-depth and is especially useful for detailed analysis and strategic decision-making.

Example 2: Targeted campaign

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 by e-mail to the H-ISAC member list, exposing the details of the campaign and relevant indicators:

- **Summary:** provides event background and relevant actor details as available
- **Analysis:** outlines harvested indicators from the specific campaign, noting details of timing and similarity of the malicious content relative to the organization the attack attempted to impersonate, including details of the attacker infrastructure
- **High Level Tools, Techniques and Procedures**: highlights key elements of the attacker content and approach in this specific campaign
- **Mitigations, Recommendations, Indicators of Compromise:** detailed steps taken to block and detect inbound attacks or outbound communications (if 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 could be provided by your organization 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: Distributed denial of service attack against an industry sector[1]

The following is a sample information sharing scenario from NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing:

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.

Conclusion

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.

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.

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

Feedback and suggestions on this document are encouraged and welcome.
Please email feedback@HealthSectorCouncil.org

[1] NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing, October 2016.
https://csrc.nist.gov/publications/detail/sp/800-150/final