45 YEARS INSA

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

JANUARY 2024

Challenges and Opportunities of Enabling Information Sharing

Presented by

INSA'S CYBER COUNCIL

Building a Stronger Intelligence Community

EXECUTIVE SUMMARY

The national security and economic prosperity of the United States depends on the public and private sectors' shared responsibility to defend its cyber infrastructure. While Federal cybersecurity policy and practice are evolving swiftly (see Executive Order 14028 and the White House's March 2023 National Cybersecurity Strategy), private sector cybersecurity remains inconsistent, leaving at risk much of our country's business and critical infrastructure. Effective information sharing is crucial for enhancing private sector cybersecurity. The shared threat information must be timely, relevant, and detailed to effectively counter cyberattacks, assist in complete system recovery, and fortify commercial networks against future breaches. This paper advocates for improved information sharing among private sector firms and provides recommendations for corporate leadership to strengthen cybersecurity measures.

Private sector firms can increase effective information sharing through operationalizing the five recommended action steps listed below. The balance of this paper provides context and details regarding their implementation.

1. Collaborate with internal stakeholders – IT, legal, compliance, etc.
   a. Establish rapport and regular touchpoints with relevant teams.
   b. Educate the workforce on information sharing processes, partners, and safeguards in place.
   c. Create an information sharing playbook and related procedures customized for each team.
   d. Conduct recurring tabletop exercises and involve all key stakeholders.
2. Improve understanding of partner priorities, collection requirements, and how recipients can action information.
3. Leverage established information sharing entities (e.g., ISACs, ISAOs) to anonymize information/intelligence sources.
4. Ensure safeguards are in place:
   a. Non-Disclosure Agreements (NDAs) or similar contractual documents.
   b. Data protection regimes.
   c. Secure mechanisms for sharing (e.g., secure portal, encrypted data feed).
5. Promote bi-directional sharing, including adopting sector-specific intelligence sharing platforms.

A one-size-fits-all solution to information sharing is less effective and inherently less secure than adopting a more tailored methodology that meets each stakeholder where they operate along a given value chain. This paper begins with an overview of existing information sharing paradigms and highlights the structural friction faced by various participants involved in these communities. A selection of best practices is then presented, drawing from both cybersecurity and counterterrorism domains. The paper concludes with a recommended information sharing methodology to be considered by the Cybersecurity and Infrastructure Security Agency (CISA), and the numerous Information Sharing and Analysis Centers (ISACs) or Organizations (ISAOs) that CISA works with to effectuate collective defense.

CYBER INFORMATION SHARING LANDSCAPE

Some private sector firms already share information with each other and the government through various ISACs or ISAOs related to their industry. Some examples of what is shared:

- Threat Actor-related – indicators of compromise (IOCs); tactics, techniques, and procedures (TTPs); forensic data; log data with only external data (no data related to the sharing firm)
- Security Best Practices – mitigations; detections/responses; interaction documents/processes such as how internal teams work together to mitigate a threat
- Current and emerging vulnerabilities and recommended mitigations
- Anomalous behavior on the networks (unusual alerts on operational technology (OT) devices, unusual hours of activity for users, etc.)

Firms generally do not share personal or confidential data, nor is there a need to, such as:

- Data the firm would consider sensitive, confidential, or secret
- Intellectual Property
- Personally Identifiable Information (PII) Data – employee or customer
- Operational impact or financial losses that resulted from a cyber incident
- Information that could identify the sharing firm if there was a data leak

BENEFITS OF INFORMATION SHARING

In general, two drivers exist for information sharing between public agencies and private companies, as well as between participants in the private sector: (i) firms who need to keep their services running as part of the nation's critical infrastructure, and (ii) those abiding by regulatory compulsion, contractual covenants, and/or insurance policy mandates.

In May 2021, President Biden issued Executive Order 14028 aimed at removing barriers to cyber threat intelligence sharing and compelling information and communications technology service providers to report cyber incidents spanning information technology (IT) and operational technology (OT) systems.[1] Also in 2021, cyber insurance premiums increased by nearly 100% year-on-year due to the rising costs of ransomware and other cyber attacks.[2] This led many carriers to reduce coverage and increase the floor for insurability. Changes to cyber insurance policies also required participants to report cyber incidents and mandated participants maintain an incident response retainer.

Organizations that deliberately engage in cyber information sharing have realized real benefits through participating in a collective defense. For example, sharing new and emerging threats within a given sector allows for greater precision in the tuning of mitigating technical solutions, mitigating controls, and security event and incident management (SEIM) monitoring. Information sharing can also result in network benefits akin to an immune system response, whereby an attack against one node in the network (i.e., a "zero day exploit") is analyzed and mitigated by all other nodes in the network before subsequent attacks can be carried out. Although quantifying the specific impacts of information sharing in an unclassified format presents challenges given security classification requirements, public-private cybersecurity collaboration has undoubtedly bolstered our national defense. The 2023 National Cybersecurity Strategy cites the disruption of the Emotet botnet as one such example of successful information sharing between public and private entities.[3,4]

Effective coordination makes the whole greater than the sum of its parts. Unfortunately, in the cybersecurity context, malicious actors have demonstrated better proficiency at coordinating with each other to maximize harm. For example, malicious actors leverage dark web marketplaces to monetize specialists' skills. In some instances, malware distributors sell access to infected devices for others to exploit. This freedom to coordinate allows threat actors to become more specialized and thereby more efficient and effective.

Coordination and sharing among cybersecurity victims and defenders has been more problematic. Obstacles presented by a wide variety of legal entities along with the lack of a common global reporting framework have slowed effective information sharing. Despite the challenges, there should be no loss of focus on the tremendous benefits that improved information sharing can bring.

> Cybercrime is no longer limited to the financial sector, due in large part to the rise in ransomware. It is therefore even more important to understand and disrupt the channels that threat actors use to move money.

Information sharing can specifically improve an organization's cybersecurity posture through:

Early warning and real-time assistance during incidents. Larger scale and faster sharing of "indicators of compromise" can mitigate the likelihood and impact of incidents. For example, ISACs/ISAOs organize communities of private sector companies to both contribute to and benefit from sharing information about suspicious activity on their IT networks. Sharing information about the origins of attacks, specific variants of malicious software, and other information allows all the participating companies to increase their readiness.

A greater understanding of the aggregate number and impact of incidents. Sizing the cybersecurity problem is impossible without seeing the problem. Yet many incidents remain hidden by victims who suffer the consequences. Maintaining confidentiality is often in the victims' best interests. But the lack of central visibility impedes the ability to understand aggregate financial impact, quantify the number of overall incidents, and study trends which can help all victims reduce their risk of a subsequent attack.

In the critical infrastructure context, this is rapidly changing. Recent legislation in the United States (the CIRCIA statute) and the European Union (NIS2) mandate timely reporting of incidents across a wide variety of sectors. The laws reflect the increased understanding that systems delivering critical services—everything from gas pipelines to food production facilities to electric grids—remain highly vulnerable. This vulnerability threatens national communications, properly functioning markets, and public confidence in the government to keep its citizens secure. Although this legislation is not all-encompassing across the private sector, it demonstrates a growing consensus about the benefits of increased information sharing.

Identification of malicious actors. Learning who is behind a cyberattack can be a difficult task, requiring piecing together forensic remnants, common victims, and infrastructure used by attackers. Increased sharing makes it easier for defenders to understand who is attacking them. This, in turn, helps defenders rapidly develop specific countermeasures, support law enforcement investigations, and publicly attribute unlawful behavior to the responsible individuals, organizations, and nations.

Tracing funds obtained by threat actors. Cybercrime is no longer limited to the financial sector, due in large part to the rise in ransomware. It is therefore even more important to understand and disrupt the channels that threat actors use to move money. Increased information sharing allows defenders and governments to identify witting and unwitting intermediaries who carry stolen funds, enable retrieval of stolen funds, and inform regulators about how to create a more transparent and accountable financial system.

BARRIERS TO INFORMATION SHARING

Both the public and private sectors face challenges in deciding how to share information without introducing additional risks or compromising the overall security posture by revealing specific cyber intelligence. Additionally, both sectors wrestle with the requirement to share information that is pertinent to the other party in a way that is actionable and prevents noise. Specific challenges faced by public-private partnerships include:

- Internal restrictions due to liability and compliance concerns about sharing with competitors or government bodies outside of regulators
- Unique industry and sector priorities and collection requirements
- Different segments within a sector (operations, supply chain, support, etc.) may need different types of information
- Risks from attribution, potential disclosure of intelligence sources, methodology, unauthorized sharing of information, etc.
- Time-sensitive nature of perishable intelligence

Even in commercial environments, certain intelligence can be used to infer sensitive capabilities/visibility. The exposure of these sources and methods can result in adversaries changing their behavior to avoid detection. Some of these capabilities can also be misconstrued in the public domain to create customer trust and public relations issues (i.e., "big brother"). Trust and successful outcomes depend on bilateral information sharing; one-sided partnerships lead to degraded results.

INFORMATION SHARING MODELS

CISA was formed "to defend against today's threats and collaborate with industry to build more secure and resilient infrastructure for the future — (it is) the public sector's steward for public-private partnerships."[5] Some sectors also have Sector Risk Management Agencies[6] (SRMAs), such as the Department of Treasury for the financial sector or Department of Energy (DOE) for the energy sector. Along with CISA and the SRMAs, the anchor cyber information sharing organizations within many sectors remain their ISAC or ISAO.[7] ISACs and ISAOs are non-profit organizations and membership is composed of vetted representatives of private industries including financial services, transportation, utilities, and other sectors. Information sharing sessions are generally closed-door and are considered a safe place to reveal sensitive findings and incidents without fear of reprisal by regulatory authorities, insurance carriers, etc. They abide by the Traffic Light Protocol (TLP)[8] to share information. The TLP levels state how the information can be further shared (if it can be shared further). The ISAC or ISAO will then act as a conduit to share information to/from CISA or their SRMA on behalf of an individual or group of firms.

In addition to ISACs/ISAOs and similar non-profit organizations, certain forward-leaning industries have begun to also demand collective defense platforms from their cyber vendors. For example, the Ad Council teamed up with leading advertisement and media fraud prevention providers to develop the HUMAN Defense Platform. This platform serves as a means of dynamically sharing new attack patterns, ranging from fake account creation (i.e., the use of synthetic identities) to automated (i.e., bot-based) media consumption.[9] Meanwhile, the DOE partnered with Dragos, an OT security provider, to establish the Neighborhood Keeper platform for sharing TTPs of cyber attackers across the utility sector.[10]

> “There is much to be learned from how government agencies without a cybersecurity mission and foreign governments share information between the public and private sectors.

There is also much that can be learned beyond the cybersecurity industry. For example, in the wake of 9-11, the future of the financial district of New York City was in question. To restore confidence in the security of Lower Manhattan, the Department of Homeland Security, New York Police Department (NYPD), and leading financial institutions partnered to create the Lower Manhattan Security Initiative (LMSI). Originally envisioned as a counterterrorism threat intelligence sharing center modeled from London’s “ring of steel”, LMSI evolved to incorporate all five boroughs of New York City and innovated a real-time information sharing platform called the Domain Awareness System. This system, in conjunction with the Lower Manhattan fusion center, served as a means by which the Joint Terrorism Task Force, NYPD Counterterrorism Bureau, and financial institutions could share real-time threat intelligence spanning declassified intelligence reports, private industry participants’ threat intelligence feeds, and sensor data.[11]

There is much to be learned from how government agencies without a cybersecurity mission and foreign governments share information between the public and private sectors. For instance, the Department of Justice conducts various outreach efforts through the U.S. Secret Service, via their Cyber Fraud Task Force in over 40 cities to “prevent, detect, and mitigate complex cyber-enabled financial crimes.”[12] Similarly, the FBI runs a program through its Office of Private Sector, designed to “protect economic and national security by strengthening the FBI’s relationships with U.S. private industry and academia.”[13] Internationally, the U.S. government maintains relationships with its allies such as the Five Eye Nations (U.S., UK, Canada, Australia, and New Zealand), European Union, Japan, etc.. The North Atlantic Treaty Organization’s Locked Shields exercise brings together the Alliance’s member states, partner nations, and select private sector partners.[14] Such exercises enable public and private sector entities across nations to share information and best practices.

RECOMMENDATIONS

As stated in the summary, the authors recommend the following for private sector firms to increase information sharing:

1. **Collaborate with internal stakeholders – IT, legal, compliance, etc.**

   a. Establish rapport and regular touchpoints with relevant teams.

   b. Provide education on information sharing processes, partners, and safeguards in place.

   c. Create an information sharing playbook and related procedures customized for each team.

   d. Conduct recurring tabletop exercises and involve representatives from all stakeholders.

2. **Improve understanding of partner priorities, collection requirements, and how recipients can action information.**

3. **Leverage established information sharing entities (e.g., ISACs, ISAOs, etc.) to anonymize information/intelligence sources.**

4. **Ensure safeguards are in place.**

   a. Non-Disclosure Agreements (NDAs) or similar contractual documents.

   b. Data protection regimes.

   c. Secure mechanisms for sharing (e.g. secure portal, encrypted data feed, etc.).

5. **Promote bi-directional sharing, including adopting sector-specific intelligence sharing platforms.**

Within firms, there are often questions from internal legal and compliance teams about what the information security team wants to share, with whom this information is being shared, and the purpose (value) of sharing. Teams in a position to share threat information should have regular meetings with their legal and compliance teams to review these matters, potentially even extending to regulatory engagement where applicable. Such engagements often start with a rudimentary review of what information security is and the role information sharing plays in collective defense. Once this common understanding is achieved, more tactical discussions can ensue, addressing how the team is leveraging its own tools, tactics, and procedures — coupled with shared information — to protect the firm from malicious activity.

Once the initial conversations have evolved, and the lawyers and compliance teams have enhanced understanding regarding the threat information and the context in which it is used, the next step would be to discuss sharing the firm's threat information. Topics to cover in these discussions can be wide ranging, but generally include:

- If there are any non-disclosure agreements (NDAs) or membership agreements in place with the organizations or firms the information would be shared with (most ISACs and ISAOs require these agreements be signed by each member);
- What information is to be shared;
- How the team can prevent the inadvertent disclosure of firm-identifying data or personally identifiable information of employees or clients;
- How this differs from information shared to regulators;
- Would the organizations you hope to share with in turn share the information with regulators; and
- An affirmation (usually involving specific incidents or details) regarding the benefits of sharing threat information as sharing increases the security of the firm, its partners, peers, and sector overall.

It is vital to be specific when describing the benefits of sharing threat information. Saying "well everyone else shares" is not sufficient. Explain how the firm's information security team uses data provided by other firms to find malicious activity on internal networks and quantify the value where possible. For example, explain (if not quantify) how shared information reduces the cost of responding to a potential incident. Also emphasize the sector-wide benefit of sharing threat information and appeal to the broader role the firm plays in this sector. Information sharing increases the collective resiliency of the sector and participation demonstrates the firm's commitment to the current and prospective customers, employees, and other stakeholders of the sector overall.

It is important to emphasize that the information being shared is strictly threat information and general best practices. There is no divulgence of intellectual property, personally identifiable information, or any similarly controlled data. Additionally, specific methods or steps taken to counter the threat are not disclosed.

Once a consensus is achieved among the stakeholders, the procedures for information sharing should be codified in a policy document and shared among other impacted teams. This policy document should outline what information will be shared and detail the process for removing any non-threat information, particularly identifying information. Additional details often included in such policies include:

- The organizations the information will be sent to;
- Approvals that will be sought by the team for each item shared; and
- Where the shared information will be housed for historical searching.

CONCLUSION

A better understanding of the benefits of information sharing and how it can be conducted effectively will improve collaboration among both public and private sector stakeholders. This in turn, supports the Department of Homeland Security's goals to increase information sharing between the government and the private sector. Moreover, it provides valuable support to firms grappling with the challenges of determining what information to share and establishing a consistent sharing process. The collective result will bolster the security posture of the nation's cyber infrastructure, contributing to a more robust and resilient collective defense.

REFERENCES

[3] *https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf*

[4] *https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation*

[5] *https://www.cisa.gov/resources-tools/resources/cisa-fact-sheet*

[6] *https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies*

[7] *https://www.nationalisacs.org*

[8] *https://www.first.org/tlp*

[9] *https://cybersecurity-excellence-awards.com/candidates/human-defense-platform*

[10] *https://www.energy.gov/sites/prod/files/2020/11/f81/CPR17_Dragos_Neighborhood%20Keeper_2020%20CEDS%20Peer%20Review_508.pdf*

[11] *https://en.wikipedia.org/wiki/Lower_Manhattan_Security_Initiative*

[12] *https://www.secretservice.gov/newsroom/releases/2020/07/secret-service-announces-creation-cyber-fraud-task-force*

[13] *https://www.fbi.gov/video-repository/ops-partnerships-072122.mp4/view*

[14] *https://www.ccdcoe.org/news/2023/worlds-largest-cyber-defense-exercise-locked-shields-kicks-off-in-tallinn*

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this paper.

INSA MEMBERS

Steve Orrin, *Chair, Intel Corporation*

Janice Haith, *Vice Chair, Oracle*

Sean Finnegan, *Workday*

Megan Foster, *TD Bank*

John Hauser, *EY*

Sydney Jones, *BNP Paribas*

Christian Schnedler, *WestCap*

Samuel Visner, *Aerospace*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Bishop Garrison, *Vice President for Policy*

Peggy O'Connor,
Director of Communications and Policy

Sam Somers,
INSA SkillBridge Fellow

Jared Chalfin,
INSA Policy Intern

Colin Hanzlik,
INSA Policy Intern

Sydney Williams,
INSA Policy Intern

Om Narayanan,
INSA Policy Intern

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 160+ member organizations and 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT INSA'S CYBER COUNCIL

INSA's Cyber Council seeks to fuse knowledge from industry, government, and academic experts in order to provide authoritative and influential insights regarding the national security challenges present in the cyber domain. The Council works to promote a greater understanding of cyber threats, challenges, and opportunities that can be addressed effectively through public-private collaboration.

45 YEARS INSA

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community