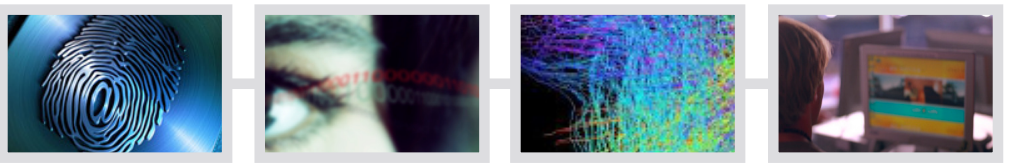
PARTNERSHIP



Cyber Information-Sharing Models:
An Overview

Table of Contents

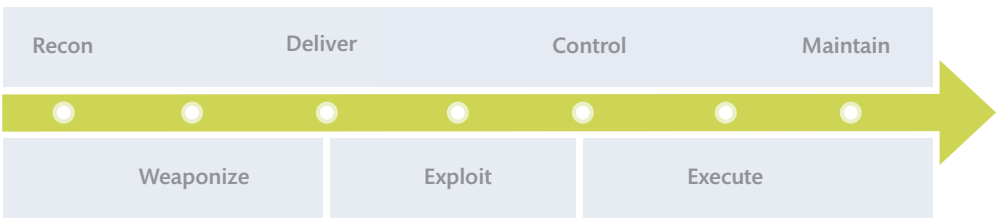
The Imperative for Cyber Information Sharing	1
Cyber Information Sharing Approaches	2
Hub-and-Spoke Models	2
Post-To-All Models	3
Hybrid Models	4
One Size Does Not Fit All	4
MITRE's Role	5

The Imperative for Cyber Information Sharing

Threats from cyber attacks are growing. Within the last year, there have been successful intrusions against several major corporations, including Sony, Citigroup, Booz Allen Hamilton, and RSA Security. The Canadian, French, Indian, and South Korean governments have all reported breaches of their computer systems and U.S. government officials have been targeted through personal email accounts. These are only the attacks that are known in the public domain; it is likely that other attacks have occurred without reaching the public eye. The consequences of such incidents are serious. Criminal groups are causing millions of dollars of damage to individuals and businesses. Adversaries are stealing valuable intellectual property and government secrets that an impact economic and national security.

One of the challenges in preventing, detecting, and responding to such incidents is that businesses and government are deeply interconnected. For instance, foreign nations may try to acquire sensitive government information by targeting companies that have government contracts. A key element in defending against these attacks is having information about the tools, techniques and resources (physical, financial, and human) that adversaries are using to breach cyber defenses. The figure below shows a framework for thinking about the methods that adversaries use to exfiltrate data from a variety of organizations.

This "kill-chain" involves a series of steps that an adversary might take to compromise, control, and exploit a target. Because similar attack methods are used throughout the kill-chain against a wide range of targets across the public-private spectrum, it is important for organizations in the public and private sectors to share information with each other. This can help organizations improve their cyber defenses and leverage the resources expended by others to improve the value of their investments. Cyber security is often expensive and the costs of intrusions can be exceedingly high; hence, there can be a massive gain in return-on-investment by leveraging work done by others. For example, the first half of the kill-chain precedes an actual exploit and represents an opportunity to proactively prevent and detect threats. The latter half of the kill-chain focuses on incident detection and response.



Cyber "Kill-Chain"

Information sharing between organizations can enable participants to develop tailored strategies for layering defenses across different steps of the kill chain. The advantages and disadvantages of sharing different types of information will be discussed in detail below.

Cyber Information Sharing Approaches

Hub-and-Spoke Models

The first formal mechanism proposed by the U.S. government to facilitate cyber information sharing was the Industry Sharing and Analysis Center (ISAC) described in Presidential Decision Directive-63 (PDD-63), which was published in 1998[1]. ISACs serve as the mechanism for gathering, analyzing, and appropriately sanitizing and disseminating private-sector information to industry and government. A center can also disseminate government information to the private sector. Although ISACs are usually designed by private sector representatives of key companies in each critical infrastructure, participation in industry ISACs is voluntary. According to PDD-63, "ISACs would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions; they would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility, and acceptability."

A number of ISACs have been created in the last 10 to15 years. Their results, to date, have been mixed. There are several reasons why many ISACs have not lived up to their potential. Many of the ISACs focus on sharing information on intrusions and vulnerabilities. Because these types of information are usually sensitive, companies are understandably reluctant to reveal this type of data to their peers and the government. Companies often choose to withhold this information; otherwise, the ISACs develop elaborate procedures to hide the identities of the organizations that do contribute this type of information. While such processes can reduce barriers to sharing, they can also slow down the information-sharing mechanism and prevent some of the face-to-face interactions that occur in trusted environments, both of which reduce the benefits of information sharing.

A related issue is that intrusion and vulnerability information is not usually actionable. In the former case, participants alert other participants after they have been compromised. Often, this is too late to mitigate attacks before serious damage occurs. In the latter case, vulnerability information is often too general to guide specific actions.

Another important issue that affects ISAC operations concerns the overall structure that is used to exchange information. Traditional ISAC models tend to rely on hub-and-spoke architectures. This type of architecture often has a central hub that receives data from the participating members (the spokes). Either the hub can redistribute the incoming data directly to other members, or it can provide value-added services and send the new (and presumably more useful) information to the members. With this approach, the hub acts as a clearinghouse that can facilitate information sharing while protecting the identities of the members. In addition, the hub may provide value by combining information from multiple members, by adding its private data, or by conducting extra analyses on the members' data.

[1] A copy of PDD-63 can be found at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (accessed August 15, 2011).

While the hub-and-spoke model has benefits, it also has limitations. The entire system relies on the functioning of the hub, which makes the system vulnerable to delays and systemic failures. If the hub is not working well, then the entire information-sharing mechanism will not work well. The more members that participate in the exchange, the more information will be sent to the hub for processing, filtering, analysis, and distribution. While more information can provide greater analytic insight, it can also increase the burden on the hub and possibly introduce delays into the system. Because the most valuable information is often time-sensitive, delays in distribution can reduce the benefits of the information-sharing mechanism. Finally, a hub-and-spoke model can be expensive. The more "value-added" services are provided by the hub, the more it will cost. If the costs are borne by the members, then those fees will become requirements for entry into the exchange. If those fees are high, they may preclude certain companies from joining the group.

A related challenge is that sharing information in this model requires a high degree of trust in the hub. It may be difficult to create a hub-and-spoke structure around either a for-profit company or a government agency. In the former case, there may be natural conflict-of-interest issues and/or members may be reluctant to share information with another company that is trying to maximize profits while acting as a trusted third party. In the latter case, companies may be reluctant to share information directly with a government agency, due to fears of information being leaked or disclosed by Freedom of Information Act requests. In addition, there are cultural barriers that often lead companies to distrust the government. Companies need to feel that the benefits they gain by sharing sensitive information with the government must outweigh the risks; often, this barrier is not crossed.

Post-To-All Models

Several industry groups and consortia have developed a different cyber information-sharing approach. This post-to-all model enables any participant to share with the entire membership roster, rather than going through a central hub. Because members share directly with each other, information dissemination is quick and can be easily scaled to many participants. A post-to-all model can also be inexpensive, because there is no need to pay for a central hub. On the other hand, this model does not contain built in "value-added" services; the only information that is flowing between members is the data collected and analyzed by the members. This places a premium on sharing the right kinds of information.

The previous section described the challenges associated with sharing data on intrusions and vulnerabilities. Such challenges would be more pronounced in a post-to-all system. The greatest benefit in either model would be derived from sharing intrusion attempt information (i.e. information about incidents, regardless of actual intrusions).

There are many good reasons for sharing intrusion attempt information:

- It is less sensitive than other types of data. Information about attempted intrusions is less revealing that information about successful intrusions. Other members will not know if the attempts were successful; therefore, they cannot draw conclusions about a given company's vulnerabilities or its information security capabilities.
- It can be disseminated quickly. Because intrusion attempt information requires less sanitization and analysis than other types of data, it can be shared quickly with other members. Timeliness is critical because adversaries adapt their tactics and techniques quickly.

- It is actionable. Intrusion attempt information can be acted upon in a timely fashion. If one organization alerts other organizations that it has detected a specific type of malware or a particular type of social engineering attack, other organizations can look for similar patterns. This can be done quickly, without revealing sensitive information to each other.

The trust issue in a post-to-all model must be handled differently than in a hub-and-spoke model. Because information is shared among participants, there must be trust relationships among all members of the exchange or the model will not work well. One way to build an atmosphere of trust is to design the information exchange to a specific mission. This will create an environment where members face common threats. They will seek to share information and focus the community around those threats. Having a specific mission makes it easier to define membership and provide direction. Furthermore, trust in a community is a function of how much members believe that other members support the same mission, respect the community rules, and are willing to participate on a reciprocal basis. Thus, building an information-sharing system for a specific mission can maximize trust, if it is implemented properly. In addition, trust is facilitated and strengthened through face-to-face meetings and individuals who have a long history of personal rapport. It is important that the information-sharing model develop vetting requirements and procedures to facilitate the introduction of new members and to maintain communication among existing members. The security, speed, and convenience of these communication mechanisms will vary with the mission and requirements of the organization.

Although it has many benefits, a post-to-all model has its own set of challenges. To scale effectively, members must agree on a common taxonomy for incident information and a template for sharing relevant information while making information anonymous and removing sensitive data. A related challenge of a post-to-all information exchange is that members must have infrastructures that protect and support the communication of relevant information and processes that allow for identifying and acting on high-priority incidents. If such infrastructures and processes place a heavy burden on member organizations, they will be reluctant to exchange information. Information security staffs are often incredibly busy; therefore, the information sharing process must be easy. That is one reason why introducing automation can be beneficial. If a company can receive an alert in a format that can be ingested and interpreted by a computer, then the people involved can focus on analyzing and evaluating response actions.

Hybrid Models

The previous sections have described two models for cyber information sharing among and between public sector and private sector organizations—hub-and-spoke and post-to-all. While these models were presented as stand-alone options, there are also blended or hybrid approaches that combine characteristics of each. For example, an information exchange could use a post-to-all architecture for the exchange of intrusion indicators while sending incident-response data to a centralized hub. This hub could conduct analysis on the data coming from multiple organizations to produce analytic reports for all to use. A second option would allow members of the information exchange to send the same data to each other and to a central hub. As before, the benefit would be the ability to act on time-sensitive data through direct, collaborative sharing while leveraging the value of the hub's ability to collect, synthesize, and analyze data across the membership and disseminate findings in the longer term.

While there are advantages to using a hybrid arrangement for cyber information sharing, disadvantages also must be considered. Establishing and running a hybrid arrangement is difficult. The mechanics of sharing information across two different architectures can become complicated, and the governance of such a model can be a challenge. In addition, the costs associated with an exchange using a hybrid model will be greater than those for an exchange that relies on a single model.

One Size Does Not Fit All

Each type of information-sharing model carries its own set of benefits and challenges. No single model will be the best choice for a given industry sector or organization. In some cases, a centralized model with value-added services may provide the most

benefits. In other cases, the ability to share information directly with peer organizations in a given industry or region may be attractive. A hybrid model may make the most sense for certain participants. Determinations must be based on a number of key factors, including, but not limited to:

- The mission of the information exchange (e.g., Is it focused on a functional area, a region, or other?)
- The number of organizations participating (present and future)
- The type of organizations (e.g., size, industry, culture)
- The role of government (e.g., If the government is involved, is it a sponsor, member, hub, or other?)
- The types of information that will be shared.

There may be cases when a single enterprise participates in multiple information exchanges, each of which has a different architecture. Regardless of the approach, cyber information sharing will not be effective unless it focuses on standardized, actionable data that can be handled in an automated manner.

MITRE's Role

MITRE brings a unique mix of attributes that make it an ideal partner for helping private or public organizations stand-up and run information sharing exchanges. The MITRE Corporation is a non-profit entity chartered to work in the public interest that operates multiple federally funded research and develop centers. As a result, MITRE often acts a trusted third party for the government and industry. For example, MITRE is the developer and custodian of multiple cyber security standards, including Common Vulnerabilities and Exposures and Open Vulnerability and Assessment Language. In this role, MITRE is sponsored by the U.S. government to lead the development of industry collaboration standards.

One benefit of MITRE's long experience working with cyber security standards is its ability to develop structures that enable the sharing and automated processing of information. This work has enabled security automation in vulnerability management, asset management, and configuration management though the Security Content Automation Protocol program. Current efforts are focused on developing structures that enable automation in malware analysis, incident response, and cyber threat sharing.

MITRE currently operates two information exchanges: one on behalf of the government and one in support of a regional research organization. The former information exchange is called the Aviation Safety Information Analysis and Sharing (ASIAS) system. It is focused on the sharing of data from airlines to improve air safety. In that model, MITRE acts as a hub that receives information from multiple airlines and the Federal Aviation Administration (FAA). Members do not share information. Each participant sends its data, which is often highly sensitive, to MITRE, and MITRE works diligently to ensure that member data is kept confidential. MITRE gathers and analyzes this information, and provides reports to all participants on key issues that affect airline safety. These reports are highly valuable, as evidenced by the growth of ASIAS from 10 to 31 members in a few years and its continued government sponsorship.

The latter information exchange is called the Advanced Cyber Security Center (ACSC), which is non-profit entity sponsored by Mass Insight Global Partnerships. ACSC focuses on information sharing among a wide range of Massachusetts-based members from industry, government, and academia. It operates a collaborative model that enables its members to share best practices, conduct and share real-time analysis, and propose new cybersecurity architectures.

Finally, MITRE is a member of multiple information sharing exchanges. Some exchanges follow the hub-and-spoke model; others use a post-to-all architecture. Thus, MITRE has first-hand experience with participating in different types of information sharing collectives. It has gathered lessons learned from its participation in these exchanges, and continuously evaluates what works and what needs to be improved in these various groups.

MITRE