Information Sharing Under CISA: What It Means For Companies

Law360, New York (February 23, 2016, 10:57 AM ET) --

Many private companies laud the information sharing system adopted by the Cybersecurity Information Sharing Act of 2015. They especially like the incentives intended to encourage the sharing of cybersecurity threat information and defensive measures that can be developed between private entities and the government.

But questions remain about the full scope of the intended benefits, and what must be done to take advantage of them. This article takes a look at some of those questions. Our next article will take a closer look at the guidelines published by the government on Feb. 16.

Why Engage in Information Sharing?

But first, a threshold question: Why engage in information sharing? The information-sharing system established by CISA is completely voluntary, so a private entity must decide to opt in. Why would a private entity do so? There are several reasons.

Chief among them is that private entities will be able to receive access to cyberthreat information shared under the auspices of CISA. Access to this information as a recipient is good in itself, since the information can be used to monitor or operate defensive measures and combat cyberthreats.

There are also benefits to providing information. Many companies are facing similar cyberthreats and in many cases are facing the same attackers. Sharing information is intended to encourage other companies to do so, thereby making more resources available to work on effective, and even collective, defenses that are deployed broadly among potentially affected companies.

CISA also authorizes the sharing of cybersecurity information between organizations without the federal
government acting as the middleman. This means that industry information sharing and analysis centers can still be used for sharing cybersecurity information and advising on threat response.

**How Does CISA Encourage Information Sharing?**

CISA offers several incentives to encourage private companies to share information.

CISA limits some of the risks associated with information sharing. For example, CISA offers certain liability protections, protects against public disclosure of the shared data and limits the government’s use of the data once it has been received.

A company that decides to share information under CISA does not waive any applicable privilege or trade secret protection associated with the information shared. Nor can the government initiate an enforcement action based on information that a company may choose to share.

So far, so good. But the devil may be in the details.

**Liability Protections**

Let’s take a look at the liability protections. Liability protection may be one of the most important incentives for companies to consider when participating in information sharing. But it may not be the shield that many think it is.

CISA offers a private entity liability protection from a cause of action (meaning, a lawsuit) for monitoring information systems. It also offers protection from a cause of action for sharing or receiving a cyberthreat indicator or a defensive measure. And it offers protection from potential antitrust violations.

The protection against lawsuits based on monitoring information systems is important. For example, it will shield companies from liability based on monitoring of their employees’ emails for cyber threat information. Similarly, companies will be shielded from lawsuits based on disclosure of information under CISA.

But there are limitations here. CISA does not shield companies from potential liability in the event of a data breach or other cyberattack. CISA is thus not a “get out of jail free” card for all manner of cyberattacks a company may suffer.

Information sharing also cannot be used to circumvent the antitrust laws. For example, information sharing cannot be used to fix prices or allocate markets or customers, which generally remain unlawful under the antitrust laws. In other words, CISA does not allow a company to do something that it already cannot do. It is not clear how much additional protection, if any, this measure adds.

**Government Oversight**

Another benefit is the limitation on the government’s use of data shared under the auspices of CISA. The federal government may use the data only to identify a cyberthreat or its source, respond to or mitigate a specific threat of death or serious economic harm, or to investigate or prosecute certain offenses specified in the law. It may not use shared data to initiate an enforcement action.
CISA requires various reporting by the government to ensure that the government stays within bounds. For example, the U.S. Department of Homeland Security must prepare a report within one year of the implementation of CISA. This report must evaluate the effectiveness of real-time information sharing, the number of cyberthreat indicators or defensive measures received through the government, and a list of federal entities that have received cyberthreat indicators or defensive measures. This reporting requirement will be beneficial to ensure that the government does not misuse shared information. How effective it will be remains to be seen.

But even if the government stays within its boundaries, companies will not be immune from government enforcement actions simply by participating in CISA-authorized information sharing. As with liability protections, companies will still be subject to the same laws requiring disclosure of breaches that they are subject to today, even if they participate in the information sharing regime.

Some Things CISA Does Not Do

As important as the things that CISA does are the things that it does not do. CISA does not:

- Require information sharing;
- Create a duty to warn based on information received through CISA’s information sharing;
- Create a federal breach notification requirement;
- Grant immunity from lawsuits in the event of a data breach;
- Grant immunity from federal government enforcement actions under existing law;
- Excuse compliance with existing reporting and notification requirements; or
- Prevent direct communication with law enforcement in the event of a data breach or other cyberattack.

Implementation Questions

To take advantage of the liability protections, information sharing must be “conducted in accordance” with CISA’s provisions. For example, data that the sharing entity “knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual” must be scrubbed from any information that is to be shared. Entities also must secure their monitoring information systems and defensive measures against unauthorized access.

CISA is expected to be implemented quickly over the coming months. The DHS published interim guidance and policies by CISA’s Feb. 16, 2016, due date, and final policies must be in place by June 15, 2016. By March 15, 2016, the DHS must certify that it has a portal capable of accepting cyberthreat indicators and defensive measures from any private entity.

These policies and procedures will guide how companies share information, and what they must do to take advantage of CISA’s benefits. Questions raised by CISA include:

- Precisely what type of information must entities remove?
- What duty do companies have to determine whether there is protected information?
• Will the federal government prescribe procedures to be used to scrub personal data?
• What will happen if a mistake is made and personal information is inadvertently shared?
• What happens if the scrubbing of this information is done improperly?
• What is the standard of care associated with scrubbing this data?
• Precisely what kind of security controls must a private entity have to ensure the appropriate data is removed?

Questions also remain on what will happen to the information after it is shared. CISA assigns the DHS the task of creating and controlling the “capability and process” (commonly referred to as a portal) through which information will be received. Before it can receive any data into this portal, the DHS must certify that it is capable of maintaining the portal. Private companies may legitimately ask whether that certification will ensure that their data will be adequately safeguarded.

Once the information is received into the portal, the information is required to be shared in real time, in an “automated” manner, with other relevant federal agencies. It is not clear from CISA what it means for the information to be shared in an automated manner.

**What to Do Now**

The CISA guidelines published by the DHS should provide helpful guidance to private entities seeking to participate in information sharing. We will review those guidelines in our next article. In addition to evaluating the guidelines, those considering sharing data under CISA can take a few steps to determine whether information sharing is right for them.

For example, companies can perform a risk analysis to determine whether to share information on cyberthreat indicators. They also can take steps to inventory potentially protected personal information that may need to be removed from any shared data. Companies can also begin developing procedures for scrubbing personal information and can review any internal controls currently in place that would ensure the security of the information received.

Although questions remain on what exactly this information sharing will look like and how effective the sharing will be, CISA offers a framework for private entities to begin considering whether information sharing is right for them.

—By Daniel Frank, Mark Thibodeaux and Allison Speaker, Sutherland Asbill & Brennan LLP

*Daniel Frank is a partner in Sutherland’s Washington, D.C., office. Mark Thibodeaux is based in Houston and deputy practice leader of the firm’s cybersecurity and privacy team. Allison Speaker is an associate in the firm’s Washington office.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

All Content © 2003-2016, Portfolio Media, Inc.