4 guidelines for cyber threat info-sharing

Department of Homeland Security releases interim guidance required by the Cybersecurity Information Sharing Act

DATA PRIVACY SOLUTIONS | MAR 14, 2016

This article is the first in a series that will discuss the DHS guidelines, with the subsequent articles diving into greater detail for each individual guideline, including what each guideline allows for. You can also find more information on CISA in our article, "What the Cybersecurity Information Sharing Act of 2015 means for your organization."

The Cybersecurity Information Sharing Act (CISA), which is the biggest piece of cybersecurity legislation passed in 2015, required the Department of Homeland Security (DHS) to provide interim guidance on how the private sector and government are to communicate threat data. DHS issued those interim guidance reports on February 16, 2016, for persons and companies sharing with the government and updates the procedures for information sharing, which include new liability protections and require the scrubbing of personally identifiable information.

THE PURPOSE OF CISA

Before we get into the specifics of those four interim guidance documents, it is important to remember why CISA proponents believe this legislation is valuable to the private sector and government. The quick answer is, in the world of cybersecurity, knowledge really is power. To mount a proper defense to a cybersecurity threat, it is important for those setting up defenses to know what they are looking for so they can properly protect against it. That principle is even more crucial in cybersecurity because hacker techniques change quickly and dramatically. In addition, they can be difficult to locate.

Most attack vectors have a telltale sign e.g., a certain type of malware they will install to infiltrate a network, the IP address of the computer from which the attack originated, or the subject line of a spear-phishing email. Knowing these things helps cybersecurity defense professionals look for these specific attack vectors before they have the ability to damage systems or breach data, and allows them to more specifically and intentionally guard against the malicious traffic.

It makes sense then that the more people who know what telltale signs to look for at any given time will make defending cyber systems easier. CISA is supposed to help in that sharing process. While the law itself did not provide any real specifics to private companies or to the government about how they could share this information and, more important, how they could share information without providing protected information or being liable for potential breach issues, it did require the DHS do so in four guideline documents.

THE PURPOSE OF THE DHS GUIDANCE

The four interim guidelines are the first steps in providing the private sector and the government with the tools to engage in this type of sharing while still protecting themselves. More to the point, in their press release on February 16, 2016, DHS Secretary Jeh Johnson noted:

> These guidelines provide federal agencies and the private sector with a clear understanding of how to share cyber threat indicators with DHS's National Cybersecurity and Communications Integration Center and how the NCCIC will share and use that information.

Johnson also pointed to DHS's Automated Indicator Sharing (AIS) system, which is an electronic sharing web portal that allows the government and private sector to share threat data in real time.

THE FOUR GUIDELINES

As for the four guidelines themselves, they offer companies a road map for sharing information while, at the same time, staying within the confines of data privacy laws, and also provides how the government is to reciprocate. Johnson noted:

> The law importantly provides two layers of privacy protections… Companies are required to remove personal information before sharing cyber threat indicators and DHS is required to and has implemented its own process to conduct a privacy review of received information.

The guidance includes four draft documents:

- Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government, which is for non-Federal (mostly, private-sector) entities on the sharing of cyber threat indicators and defense measure;
- Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities, which is for federal entities on the sharing of cyber threat indicators and defensive measures;
- Interim Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government, which is related to the receipt of information by the federal government, and
- Privacy and Civil Liberties Interim Guidelines

With respect to the guidance for the private sector, the manner in which the information is shared affects the protections available for sharing cyber threat indicators and defensive measures. Some sharing receives liability protection and some does not. Private entities should make sure they are sharing information correctly to ensure they are getting the most protection from liability under the law.

4 guidelines for cyber threat info sharing

The Federal Register notice from DHS is available here.