CARLTON FIELDS

Share What You Know: Liability Protection for Private Entities that Share Cybersecurity Information Pursuant to Federal Guidelines

June 02, 2016

On February 16, the Department of Homeland Security (DHS) and the Department of Justice (DOJ) jointly issued preliminary guidance — with final guidance due later this month — on how the private sector and government will communicate cyber threat data and defensive measures under the Cybersecurity Information Sharing Act (CISA). Enacted at the end of 2015, CISA aims to help swiftly identify and mitigate potential cyber incursions. It provides liability protections to private entities that monitor information systems and employ defensive measures to address cyber threats to those systems. CISA also encourages industry to share with the federal government cyber threat indicators and defensive measures deployed in response to those threats. Specifically, CISA provides that no cause of action can be brought against private entities that conduct activities authorized by and in accordance with the Act. CISA offers other incentives for information-sharing. For example, it makes clear that information shared with the government retains applicable legal privileges and protections, including trade secret protections and exemptions for disclosure and antitrust laws. CISA directed the Executive Branch to develop guidelines and other procedures to implement the Act. Accordingly, the DHS and DOJ issued instructions for sharing cyber threat indicators and defensive measures with DHS's National Cybersecurity and Communications Integration Center (NCCIC). The guidance explains how NCCIC will share and use that information, and provides helpful examples of what may or may not be shared. In particular, the guidance states that it is permissible to share information "directly related to and necessary to identify or describe a cybersecurity threat." Expanding on this concept, the guidance clarifies that "[i]nformation is not directly related to a cybersecurity threat if it is not necessary to assist others detect, prevent, or mitigate the cybersecurity threat." For example, in the context of a spear phishing email, the guidance explains that the sender's email address could be considered directly related to a

cybersecurity threat, but personal information about the target (the recipient email address) typically would not meet that standard and should not be included. Four mechanisms are available to private entities that wish to take advantage of CISA's liability protections: (1) DHS's Automated Indicator Sharing (AIS) system; (2) a fillable web form; (3) email to NCCIC; or (4) through Information Sharing and Analysis Centers or Information Sharing and Analysis Organizations. The guidelines also explain how to identify certain types of personally identifiable information that must be removed from any data before it is shared with the government. To be clear, liability protection is only given under CISA when information is shared with NCCIC by one of the four methods above, and only if the data is scrubbed of personal information before it is shared. Although CISA allows information sharing outside of NCCIC, it must be for a cybersecurity purpose, and even then, such sharing does not enjoy CISA's liability protections. Although initially heralded as a significant piece of legislation, CISA's impact remains to be seen. Indeed, a recent survey of global IT professionals found nearly three-quarters of U.S. respondents stated they are in favor of CISA, thus recognizing the value of information sharing among businesses, government, and consumers. Yet, given corporate-reputation concerns, less than half believed their own organization would voluntarily share cyber threat information after a breach. Beyond corporate-reputation concerns, public companies may also be wary of sharing information pursuant to CISA, lest such reporting also trigger disclosure obligations in the view of the Securities and Exchange Commission. Only time will tell whether CISA and its implementing guidance have sufficiently encouraged greater cybersecurity information sharing to overcome the private sector's general reluctance. If nothing else, companies should be mindful of their options under CISA, and factor it into their incident response plans.

Authored By

Erin J. Hoyle

Related Practices

Cybersecurity and Privacy
Intellectual Property
Technology

Related Industries

Technology