Recent government action has shown that the White House and Congress are keenly aware of the potential data security benefits of robust information sharing between and among the private sector and the government. Last year, President Barack Obama unveiled an executive order (EO) to improve the cybersecurity of critical infrastructure entities that highlighted the important role information sharing must play. In recent years, information sharing bills have been introduced regularly in both the Senate and the House, and again on July 10, Sen. Dianne Feinstein, D-Calif., introduced the Cybersecurity Information Sharing Act of 2014 (CISA) in an effort to encourage the flow of cyberthreat data between the private sector and the government.

Companies are already sharing cyberthreat data, but many remain leery as they engage in this largely unchartered territory. This article will analyze the primary concerns raised by companies and highlight steps they can take to safely share information and leverage this important weapon against cybercrime.

The Benefits of Sharing

Receiving critical threat data has been shown to be an effective tool in both preventing cyberattacks and mitigating the effects of ongoing attacks. In a recent study, PricewaterhouseCoopers found that 82 percent of companies with “high-performing security practices collaborate with others to deepen their knowledge of security and threat trends.” IT security professionals also understand that information sharing is an integral part of defending their company from cyberattacks. Their belief is warranted, as last year one of the most highly respected information sharing platforms, the Financial Services Information Sharing and Analysis Center (FS-ISAC), was able to significantly mitigate the effects of a cyberattack on the sector by analyzing threat information it received from some of its members and quickly pushing it out to other financial institutions. In July, the concrete benefits of information sharing made headlines when the retail unit of a Fortune 100 company announced that it discovered malware on its system as a result of receiving threat intelligence from a government advisory. As those examples show, threat data is pushed out to companies from a variety of sources stemming from both the private sector and government.

As information sharing has increas-
ingly been lauded as an effective tool in combating cyberthreats, the available platforms and methods for sharing such information have grown. Information security professionals have long relied on informal and semistructured networks and relationships with individuals in peer organizations to gain better insight into cybersecurity threats and vulnerabilities. While informal sharing remains the most common method, more formal mechanisms and platforms are gaining traction.

One mechanism, the post-to-all model, is similar to listservs. Organizations can post information regarding a cybersecurity incident to a message board or send out an email to a large group. In another model, certain business sectors have pooled their resources to create or join existing information sharing and analysis centers (ISACs), such as FS-ISAC. ISACs are sharing platforms designed to streamline the collection, analysis and dissemination of threat intelligence within a given sector. They follow a hub-and-spoke model in which companies send cyberthreat data to a common hub that organizes and analyzes the data before sending actionable threat intelligence out to ISAC members. Critical infrastructure sectors such as banking, energy and telecommunications have developed ISACs to more efficiently leverage threat data. An added benefit of ISACs is that they can become established, trusted entities with which the government feels comfortable sharing its valuable threat intelligence.

The government is a particularly useful source of threat data, in part because it obtains intelligence from such a wide variety of sources, be it law enforcement investigations into hacking groups, intelligence gathering activities or agencies monitoring their own systems for signs of cyberthreats. In 2009 the U.S. Department of Homeland Security (DHS) created the National Cybersecurity and Communications Integration Center (NCCIC), which is essentially a central repository of the critical threat data known to the government at federal, state and local levels. NCCIC works in collaboration with many ISACs to provide this trove of information to the private sector so that companies may better defend themselves from cyberattacks. Since the administration released the EO on protecting U.S. critical infrastructure last year, NCCIC has become a more visible and active entity that is now the primary gateway through which the private sector interacts with the government to share and receive threat data.

Mitigating the Risks

The threat data shared through information sharing mechanisms is not the type of business-sensitive or private information that some companies may envision. Information sharing programs are designed to distribute “actionable threat intelligence,” such as technical data that an organization’s information security team can use to prevent, detect or block an attack. The core of that threat intelligence is cybercriminals’ tactics, techniques and procedures (TTPs).

TTPs are the behaviors and modus operandi of cybercriminals that shed light on how they compromise and exploit systems. TTPs include not only information related to a cybercriminal’s attack pattern, but also the tools and IP addresses they use to carry out attacks, as well as specific technical data on the malware they inject into systems. Such threat intelligence is therefore distinct from the type of sensitive personal information that can be targeted in cyberattacks. While sharing sensitive personal information with other companies could reasonably raise privacy and potential liability concerns, sharing only technical threat intelligence carries far fewer risks. Indeed, many information sharing mechanisms take steps to ensure that sensitive personal information is not shared or disclosed.

ISACs as well as other formal and informal mechanisms create sharing tools and implement operational rules designed to assuage fears related to information sharing. Companies often are allowed to share information anonymously so that the technical data shared with other members cannot be ascribed to that company. Additionally, companies may sometimes specify that any information they share will be disseminated only to other members, and not to outside entities such as the government. Some platforms also create varying levels of membership that allow companies to share information only with certain entities, such as those approved as trustworthy by multiple independent sources or those that are more actively engaged in the platform. While these protections address some concerns, the government also has taken proactive steps to remove barriers to sharing by issuing statements on how it interprets particular laws that companies worry could be violated when they share threat data.

Recently, the U.S. Department of Justice (DOJ) sought to address the commonly expressed concern that information sharing runs afoul of the various state and federal privacy laws governing the collection, storage, use and disclosure of certain types of information. Recognizing that companies were concerned over this issue in one particular context applicable to online service providers, the DOJ released a white paper announcing its interpretation of how information sharing interacts with the Stored Communications Act (SCA), which prohibits the disclosure of certain consumer information. According to the DOJ, cyberthreat data may be shared with the government as long as any consumer information is in “aggregate form” so it cannot be connected to a single individual. The white paper underscores that, in general, individual consumer information is not useful threat data; actionable threat intelligence is distinct from the type of information that companies have been hesitant to disclose due to privacy concerns.

Companies also have worried that sharing cyberthreat data could be interpreted by government regulators as
Anticompetitive behavior. The DOJ and the Federal Trade Commission recently released a policy statement on the issue. The agencies announced that their real concern was the sharing of competitively sensitive information such as "current and future prices, cost data or output levels." Their policy statement recognized that the type of technical data involved in information sharing programs generally is unrelated to such competitively sensitive information, and as such the sharing of cyberthreat data "is not likely to raise antitrust concerns."

While the government has proactively minimized antitrust and (some) privacy law concerns, it has yet to address other issues, such as protecting shared data from public disclosure, and abating fears surrounding regulatory use of shared information or civil liability resulting from information sharing. Companies also have expressed concerns that proprietary or confidential data will be discoverable through Freedom of Information Act (FOIA) requests. Currently, there is a mechanism to share information with the government while shielding it from FOIA, albeit in a narrow context. Congress and DHS created the Protected Critical Infrastructure Information program, which grants broad statutory protection to certain cyberthreat data shared with DHS. However, the program is applicable only to critical infrastructure entities sharing "critical infrastructure information"; the extra step of filtering data through, and complying with the requirements of, the program is an additional layer of process that may defeat the purpose of near real-time information sharing.

Other areas of concern are regulator use of shared information or civil liability resulting from information sharing. Throughout a security incident or data breach investigation, companies are bound to engage with various government officials, each with their own agendas. Companies that are victims of cybercrime will almost invariably work with law enforcement agents hoping to catch the criminals, or with intelligence officials working to understand the threat. At some point a security incident may become public (particularly if customer or personal information is involved) through a required notification to customers, a public filing or the naming of a victim in an indictment. When this happens, the company can expect to receive an inquiry from a federal or state regulator, or both. Regulators may ask the company to provide them with the information the company provided to a different arm of the government.

Companies should understand that regulators often cannot obtain this same information from law enforcement (it may be protected, for example, by grand jury secrecy restrictions). To the extent that companies suspect that the sought-after information may be used against them (i.e., the timing of having knowledge of the event), companies should push back appropriately, pointing to the administration’s firm position of encouraging the free flow of information between the government and the private sector, which is undermined by regulators using this information against companies actively engaged in cooperative efforts to reduce threats.

Similarly, victims of cyber-incident are wary that without safe harbor or liability protections, plaintiff’s counsel may use shared threat as the basis of, or to strengthen, civil lawsuits against companies err on the side of providing threat data to ISACs or listservs by taking comfort that private companies are not subject to FOIA, and recognizing that certain risks can be mitigated by taking advantage of the tools these mechanisms offer to share information anonymously and stripped of sensitive, personal information.

Information sharing is a relatively inexpensive data security measure, but it can be a crucial tool in preventing costly, image-damaging cyberattacks. Just as cybercriminals work in tandem to identify weaknesses and infiltrate corporate networks, companies and the government should work together to share information, strengthen their defenses and reduce the success of cyberattacks.

Kimberly Peretti is a partner at Alston & Bird in Washington, D.C. She is a member of the firm’s white-collar crime group and co-chair of the security incident management and response team. Lou Dennig is an associate in the firm’s litigation and trial practice group and also is a member of its response team.

The Bottom Line
Despite the lack of robust FOIA protections or protections against regulator use of shared information, companies should make information sharing their default position. The potential and proven benefits of sharing threat data far outweigh the potential risks. Upon receiving requests from the government to share information, companies should keep in mind that, depending on the form of the request and the agency making it, shared data could be protected from further disclosure or use in a civil action. In the absence of such protections, companies should request a confidential or business-sensitive FOIA exemption, or oral or written assurances that shared information will not be disclosed further.

In terms of private sector sharing, companies should err on the side of providing threat data to ISACs or listservs by taking comfort that private companies are not subject to FOIA, and recognizing that certain risks can be mitigated by taking advantage of the tools these mechanisms offer to share information anonymously and stripped of sensitive, personal information.