Cooley

April 14, 2014

The scenario: your CSO is on the line. This time, she says, it was a spear phishing attempt—emails individually addressed to a few employees, each with an attachment deceptively titled to resemble a standard invoice. She tells you the good news: your network security team caught the messages in time. They quickly identified the source IP and email addresses and blocked additional messages before they hit inboxes. You find out later other companies were also targeted, but no one talked until it was over.

The challenge: Timely threat information—like the IP and email addresses used for spear phishing—can be critical to cyber attack prevention, containment and response. But without effective information sharing, multiple companies targeted by the same or similar threats may each be left scrambling to fend for itself as an attack unfolds in real time.

On Thursday, the Department of Justice (DOJ) and the Federal Trade Commission (FTC) responded to claims that antitrust worries have been stopping companies from sharing cyber threat information, especially with competitors. In a joint statement, the two agencies assured companies that antitrust should not represent a "roadblock" to cybersecurity information sharing arrangements.

According to the statement, such arrangements are "very different from the sharing of competitively sensitive information such as current or future prices and output or business plans which raise antitrust concerns." The antitrust enforcement agencies recognize that cyber threat information sharing is usually "procompetitive".

The statement does not represent a change in antitrust policy. Instead, it reaffirms guidance issued in October 2000 in a business review letter to the Electronic Power Research Institute (EPRI), in which the DOJ concluded that EPRI's plan to share physical and cyber threat information among competitors was likely to result in more efficient means of reducing cybersecurity costs and savings would redound to the benefit of consumers. Friday's statement served to clarify and expand upon the analysis in that 2000 letter.

Specifically, the statement green-lights most arrangements to share technical cybersecurity information, and provides certain representative examples. These include:

- Incident or threat reports
- Alerts of security threats or activity
- "Indicators" of attacks, such as file hashes, computer code, URLs, source email addresses and technical characteristics of malware
- "Threat signatures," defined as "the characteristics of specific cyber threats that may be used (often by automated systems) to identify, detect, and/or interdict them"

Moving forward, companies should define an internal policy that articulates what should and should not be disclosed before entering into a cyber threat information sharing arrangement. Because price and other competitively sensitive information may be targeted or otherwise implicated in a cyber attack, internal protocols should provide for the exclusion of any such data from sharing.

For further information, contact one of the attorneys listed above.

assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Matthew D. Brown **San Francisco**	**brownmd@cooley.com** **+1 415 693 2188**
Howard Morse Washington, DC	hmorse@cooley.com +1 202 842 7852
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090