Bloomberg BNA

Antitrust & Trade Regulation Report™

PRIVACY

Cybersecurity

DOJ and FTC Help Pave the Way For Greater Cyber Information Sharing in the Private Sector




BY DAVID LAING, EVAN D. WOLFF, ELIZABETH BLUMENFELD AND KATE M. GROWLEY

Defending against cyber attacks is becoming an all-consuming task for companies. Nearly every day, newspapers announce a new U.S. company that has been hacked. With customer or employee personally identifiable information (''PII'') or the companies trade secrets the target, U.S. companies across industry sectors are facing increasing threats from not just Chinese state actors but also Russian and Iranian hackers.

One need not look any further than the highly publicized Target breach to understand the corporate implications of an unsuccessful cyber defense. Through an unwitting services vendor, cyber attackers furtively accessed Target's internal network and managed to steal the financial and personal information of up to 110 million customers. The public backlash has been palpable and has exposed the retail powerhouse to potentially years of litigation and hundreds of millions of dollars in associated costs. Lawsuits against Target run the gamut, including litigation brought by banks, credit unions, shareholders, and individuals whose information was stolen. The damage done to customer and partner confidence likely cannot be quantified.

But as scary as these repercussions sound, what is even scarier is that Target is not the first and certainly will not be the last to suffer such a breach. Since the Target incident, other prominent companies like Neiman Marcus and eBay have come forward to announce their own breaches. And so, faced with this new reality that mitigating computer crime has become a cost of doing business, companies are scrambling to find new ways to avoid becoming the next ''target.''

Increasingly, companies are adding the use of information sharing to their arsenal of defenses. They are realizing that knowledge is power, and cyber attacks are no exception. For example, if Target had been sharing vulnerability information with other retailers, it may

Based in Washington, D.C., **David Laing** *is a partner in Crowell & Moring's Antitrust Group.* **Evan D. Wolff** *is a partner in the firm's Government Contracts Group and in the Privacy & Cybersecurity practice, which he helps lead.* **Elizabeth Blumenfeld** *is a counsel in the firm's Privacy & Cybersecurity Group, and* **Kate M. Growley** *is an associate in the firm's Privacy & Cybersecurity, Government Contracts, and Litigation Groups.*

 ISSN 0003-6021

have known to scrutinize its vendors' access to its networks and thwarted the breach before its customers' information was stolen. What one company can amass about the cybersecurity battlefield pales in comparison to the cumulative knowledge that multiple companies fighting on the same front can amass. With cybersecurity data sharing, the whole can be more than the sum of its parts. With the advent of big data analytics, companies can distill more helpful insights from the aggregate information collected across its industry. In contrast, companies that attempt to defend their networks without the benefit of robust information sharing are unlikely to succeed. Put simply, they will know too little, too late.

Despite its significant benefits, cyber information sharing is not without its risks. At first glance, those associated with the unintended disclosure of information beyond the target network come to mind. Threat actors can exploit a company's disclosed vulnerabilities against it. Customers or business partners may lose confidence in a company's cybersecurity capabilities. Disclosures may initiate regulatory investigations of a company's apparent failure to comply with cyber best practices. Or a company may have to contend with an unintentional disclosure of trade secrets or PII.

But for private companies, a more fundamental risk stems from the nature of information sharing itself – violating antitrust law. Fear that the federal government might consider such information sharing as a ''restraint on competition'' between companies that are competitors, and thus potentially violate the Sherman Act, could prevent companies from otherwise taking advantage of the benefits of industry-wide cybersecurity information sharing. In fact, the ABA's Standing Committee on Law and National Security — known for its strong cybersecurity advocacy — is one of many organizations that have commented on the antitrust concerns that cyber information sharing raises. ''Antitrust concerns have triggered suspicion about close coordination among corporate competitors, including discussions of cybersecurity information sharing.'' [Standing Committee on Law & National Security, A PLAYBOOK FOR CYBER EVENTS 59 (American Bar Association) (2013) (hereinafter, ''CYBER PLAYBOOK'').] The Committee, however, has also drawn attention to prior Department of Justice (''DOJ'') comments suggesting that antitrust law and cyber information sharing are not irreconcilable, provided that the latter thoughtfully accounts for the former. Recent events have confirmed the ABA's sound advice.

In light of the growing number of companies looking towards information sharing as a cyber defense strategy, the DOJ and the Federal Trade Commission (''FTC'') have clarified their positions on how it may implicate antitrust concerns. On April 10 of this year, both agencies issued a joint statement entitled ''Antitrust Policy Statement on Sharing Cybersecurity Information'' (''Cybersecurity Antitrust Statement'') that provides America's private sector with the clarity it needs to share cybersecurity information without violating the antitrust laws that the DOJ and FTC enforce.

Recognizing the benefits of cyber cooperation, the antitrust agencies made clear that they ''do not believe that antitrust is — or should be — a roadblock to legitimate cybersecurity information sharing.'' Indeed, ''properly designed cyber threat information sharing is not likely to raise antitrust concerns and can help secure the nation's networks of information and resources.'' The agencies' emphasized that, in order to be ''properly designed,'' information shared as part of collaborative cybersecurity efforts should not contain ''competitively sensitive information – such as recent, current, or future prices, cost data, or output levels.'' Information exchanges that have the purpose of providing collaborative cybersecurity and that are limited to technological efforts to detect or protect against intrusions will raise no concern for the antitrust agencies.

Helpfully, the agencies provided specific examples of what information can be freely shared without raising antitrust issues. Malware signature detections, suspicious IP addresses, or common DDoS target portals typically do not contain competitively sensitive information that would raise the agencies' eyebrows. As such, the sharing of this cybersecurity information, even between direct competitors, would likely not create any material possibility of an antitrust investigation, as long as the competitors did not also exchange information that might affect their competition such as product pricing, decisions on output or production levels, or terms of sale to customers.

In many ways, the Cybersecurity Antitrust Statement affirms enforcement policies that the two federal antitrust agencies have articulated previously. Almost fifteen years ago, the DOJ issued a business review letter to a non-profit organization named the Electric Power Research Institute (''EPRI''). [*See* Letter from Joel I. Klein, Asst. Att'y General, Antitrust Div., to Barbara Greenspan, Assoc. General Counsel, EPRI (Oct. 2, 2000).] Because EPRI disseminated technology-focused solutions to the energy sector, it sought guidance from the DOJ Antitrust Section regarding the antitrust implications of its collaborative infrastructure security efforts. Specifically, EPRI had devised an information exchange that could reduce the risks associated with the energy sector's increased reliance on technology and computer interconnectivity. Concerned about how the Antitrust Section would view the proposed information exchange, EPRI queried the DOJ about its enforcement intentions. In line with the DOJ and FTC's current position, the Antitrust Division in 2000 determined that the energy sector's exchange of information related to best practices and cybersecurity vulnerabilities would not present antitrust concerns because it would not restrict competition in the energy-related markets. Again, the information exchanged within the sector was to be limited to only physical and cybersecurity issues. Notably, any discussions regarding competitively sensitive information – such as price, purchasing, or product innovations – were to be excluded from the exchange.

More recently, the DOJ echoed that its position articulated in the EPRI Letter remained its position today. That is, although the DOJ's guidance to EPRI is ''now over a decade old, it remains the Antitrust Division's current analysis that properly designed sharing of cyber-security threat information is not likely to raise antitrust concerns.''

That the DOJ and FTC took the uncommon measure of reaffirming its prior position by jointly stating an enforcement policy in the Cybersecurity Antitrust Statement is one more example of how the federal government is – without legislation – encouraging greater cybersecurity in the private sector. For example, President Obama signed Executive Order 13636 on ''Improving Critical Infrastructure Cybersecurity'' over

  ATRR ISSN 0003-6021

a year ago. In addition to the often-cited voluntary standards that it spearheaded, the Order emphasized that the security of the nation's IT infrastructure relies, in part, on the private sector's willingness to share cybersecurity information. The Cybersecurity Antitrust Statement is one more step towards achieving that objective.

Hearteningly, many industries have already created their own sharing networks that focus on their core cybersecurity concerns, without sharing the kind of competitively sensitive information with which U.S. antitrust laws are concerned. The most common of these networks are known as Information Sharing and Analysis Centers (''ISACs''). [CYBER PLAYBOOK at 59 n.152.] Largely, ISACs serve as kind of clearinghouse for technical information, across a variety of industries, including financial services, communications, electric, emergency response, and national health.

Of these, the Financial Services ISAC (''FS-ISAC'') is considered the most mature. [CYBER PLAYBOOK at 60 n.154.] Coincidentally, it is also an excellent example of how an ISAC can function within the bounds of the DOJ's antitrust guidance. The FS-ISAC outlines a specific set of Operation Rules with which all members must comply. For example, all submissions must be anonymous; information sharing must be authenticated; the ISAC must at all times be industry owned and operated; and it does not allow external access through Freedom of Information Act (''FOIA'') requests. These underlying principles work to the benefit of the FS-ISAC members, while mitigating the risk that it will facilitate the sharing of sensitive corporate information among competitors.

Importantly, other industries are taking note of the FS-ISAC's approach to information sharing. Partly in response to the growing frequency of incidents such as the Target breach, the retail industry has announced that it is developing — in coordination with the FS-ISAC — its own retail ISAC (''R-CISC''). Hoping to capitalize on the FS-ISAC's lessons learned, the President of the Retail Industry Leaders Association has explained: ''Retailers place extremely high priority on finding solutions to combat cyber attacks and protect customers. In the face of persistent cyber criminals with increasingly sophisticated methods of attack, the R-CISC is a comprehensive resource for retailers to receive and share threat information, advance leading practices and develop research relevant to fighting cyber crimes.'' By modeling the R-CISC after the FS-ISAC, the retail industry will also help to alleviate the antitrust risks inherent to information sharing of any kind.

At the end of the day, the decision to participate in an information sharing network will be a strategic one, based on both the benefits and the risks. As the success of the FS-ISAC and growth of the R-CISC illustrates, it is a strategy that private companies are more and more inclined to adopt. As the private sector faces mounting threats from cyber criminals, the DOJ and FTC Cybersecurity Antitrust Statement will at least help ensure that antitrust liability is low on these companies' lists of cyber concerns.