[Industry Collaborations on Cybersecurity]

</Protecting Against Antitrust Violations>

By Evan Wolff, David Laing, Elizabeth Blumenfeld, and Kate M. Growley

May 2014 found the Department of Justice (DOJ) with a first: criminal charges brought against a state actor for computer hacking, economic espionage, and other offenses. In the Western District of Pennsylvania, a grand jury indicted five members of the Chinese military for conspiring to hack into the computers of American corporate behemoths such as Westinghouse Electric Co., US Steel Corp., and Alcoa, Inc.—all to steal trade secrets that would benefit Chinese competitors, including state-owned enterprises. According to US Attorney General Eric Holder, "[t]he range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response." (Press Release, Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), http://tinyurl.com/oyxmb44.)

Although the indictment itself may have come as a surprise, the story behind it is all too familiar to American industry in the twenty-first century. Computer hacking—including that committed in the name of economic espionage—is prolific and increasing. The Chinese indictment has drawn public attention for its notable and unprecedented suspects, but it remains just one of dozens of hacking prosecutions that the DOJ has pursued in recent years. (*See, e.g.*, Press Release, Dep't of Justice, Texas Man Convicted in Corporate Hacking Case (Mar. 1, 2013), http://tinyurl.com/axgrs82; Press Release, Dep't of Justice, Leader of Hacking Ring Sentenced for Massive Identity Thefts from Payment Processor and U.S. Retail Networks (Mar. 26, 2010), http://tinyurl.com/p8avfxh.) Faced with the new reality that computer crime is a cost of doing business, companies are scrambling to find new ways to avoid becoming victims.

One method picking up steam is information-sharing between similar companies. Knowledge is power when it comes to cyber-attacks. And a company's ability to understand its vulnerabilities and the potential threats seeking to exploit those vulnerabilities is its first line of defense against today's pervasive cyber risks. Realistically, though, there is only so much information that a single company can amass, and limited data renders limited insights. Combining data from many companies creates the potential for something profoundly more useful. Similar to how crowdsourcing takes advantage of the willingness of online communities to accumulate and analyze troves of information, industries that share cyber-threat information can aggregate data from a larger pool of resources. The result is a communal capacity to spot and counter trends, often before any single company would be able to on its own. Just as malicious actors commonly share information with one another to evade their targets and law

Evan Wolff, David Laing, *and* **Kate M. Growley** *are attorneys in Crowell & Moring's Washington, D.C., office. Wolff is a partner and co-chair of the firm's Privacy & Cybersecurity Group and served as an advisor to the senior leadership at the Department of Homeland Security and other US government agencies on cybersecurity issues. Laing is a partner in the firm's Antitrust Group and a former trial attorney in the US Department of Justice, Antitrust Division. Growley is an associate in the firm's Privacy & Cybersecurity Group.* **Elizabeth Blumenfeld,** *recently counsel with the firm, left that position to become executive director of Heart Healers International, a nonprofit organization that provides heart surgeries for children in Sub-Saharan Africa.*

Published in Criminal Justice, Volume 29, Number 3, Fall 2014.

enforcement, so too must those targets vigilantly share their cyber awareness among themselves to effectively adapt in the face of those actors. The breadth and timeliness of the insights that these communities can achieve are critical to their ability to stay one step ahead of, or at least not too far behind, the malicious actors. As the American Bar Association's (ABA's) Standing Committee on Law and National Security noted in its 2013 publication, *A Playbook for Cyber Events* [hereinafter Cyber Playbook], organizations that attempt to defend their networks without such information-sharing are unlikely to succeed. They will know too little, too late.

Yet this need for industry-wide collaboration comes at a time when the United States has been actively investigating and prosecuting other forms of information-sharing. In these instances, the DOJ has argued that such collaboration is a criminal antitrust violation of the Sherman Act of 1890. (15 U.S.C. § 1.) This has occurred most recently and most notably in the financial services industries, including DOJ investigations and prosecutions in the LIBOR (London Interbank Offered Rate), foreign currency exchange, municipal bond, and credit-default swaps areas. Fines and related penalties have been substantial. UBS AG companies pleaded guilty to antitrust violations related to LIBOR and paid total penalties of more than $1.5 billion in 2012, including penalties imposed by the Commodity Futures Trading Commission, as well as the UK and Swiss financial services regulatory agencies. Rabobank agreed to pay total penalties exceeding $1 billion in the LIBOR investigations; Royal Bank of Scotland PLC companies agreed to pay total penalties of approximately $612 million. (*See* Press Release, Dep't of Justice, Rabobank Admits Wrongdoing in LIBOR Investigation, Agrees to Pay $325 Million Criminal Penalty (Oct. 29, 2013), http://tinyurl.com/mg7bua4; Press Release, Dep't of Justice, RBS Securities Japan Limited Agrees to Plead Guilty in Connection with Long-Running Manipulation of LIBOR Benchmark Interest Rates (Feb. 6, 2013), http://tinyurl.com/bbbwy9w; Press Release, Dep't of Justice, UBS Securities Japan Co. Ltd. to Plead Guilty to Felony Wire Fraud for Long-Running Manipulation of LIBOR Benchmark Interest Rates (Dec. 19, 2012), http://tinyurl.com/c3ae3wp.)

Some defendants in these antitrust investigations are raising, as part of their defense, arguments that the information-sharing was necessary to allow the markets to exist or function, not the criminal antitrust violation that DOJ asserts. The line between lawful information-sharing among competitors and an "agreement in restraint of trade" that violates the Sherman Act can at times be difficult to discern. This article discusses best practices to help assure that industry-wide cybersecurity collaboration remains clearly on the right side of that line.

Information-Sharing in Cybersecurity Efforts

Generally, there are two categories of information that aid in thwarting cyber-attacks. The first relates to hardware and software vulnerabilities. Not surprisingly, this information tends to originate from hardware and software vendors themselves, along with other government research and analysis centers, nonprofit groups, and cybersecurity firms. (Cyber Playbook, *supra*, at 53–54.) For example, Microsoft releases updates for its Windows operating system on the second Tuesday of every month. Over time, corporate entities have come to anticipate and rely on these updates, issued on what is now commonly known as "Patch Tuesday." By providing companies that use Windows with a set time for these updates, Microsoft is easing what could otherwise be erratic notifications and costly scrambles to patch important vulnerabilities.

The second type of information is the threat information itself. Focusing on the malicious actors or their techniques, this information originates not only from the same groups as above, but also from other companies within the same industry, law enforcement, and intelligence agencies. (*Id.* at 54.) Probably the most well-known instance of threat information-sharing is last year's report by cybersecurity firm Mandiant, which illustrated how a certain Chinese military unit was likely responsible for over 100 corporate infiltrations and the subsequent theft of significant intellectual property. (Mandiant, APT1: Exposing One of China's Cyber Espionage Units (2013) [hereinafter APT1 Report], *available at* http://tinyurl.com/bjnsvjo.) The report's publication, and extensive distribution, accomplished several things. First, the *APT1 Report* provided valuable information regarding the actor's identifiers, such as malware profiles and IP addresses, as well as its techniques, such as compromised encryption certificates. (*Id.*) The *APT1 Report* also notified unsuspecting victims about the infiltrations and put potential targets on notice. More importantly, the report drew a roadmap for others looking to share similar threat information. The *APT1 Report* spurred hundreds of similar reports that shed even more light on this and other threats. (*See* Cyber Playbook, *supra*, at 54 n.143.) Of course, the report also tipped off the malicious actor that its secret was out. The presumed result was that the Chinese unit and others using similar schemes migrated to new tactics. But that migration incurs costs. As such, arguably the most significant role that the *APT1 Report* played was to increase the costs of doing business for cybercriminals.

Those increased costs are one example of the benefits of amassing and sharing cyber-threat information across an industry. Doing so allows organizations to mitigate cyber risk by reducing overall volume, severity, and frequency of cyber incidents, while increasing internal cyber preparedness. Importantly, information-sharing comes at a comparatively low cost. Rather than expensive investment in independent research and development, companies can learn from each other's cyber triumphs and failures. This, in turn, enables those companies in an information-sharing relationship to invest in their most pressing cyber concerns. Even the determination of what those concerns should be will likely be informed by shared information. The scaled benefits of information-sharing make this preventative tactic all the more appealing to small or less sophisticated businesses, whose systems have been particularly alluring targets for cybercrime. (Cyber Playbook, *supra*, at 56 n.149.)

The benefits of cyber collaboration can also be less immediately tangible. Greater cybersecurity leads to a lesser chance that a company's name lands itself in the headlines. Similarly, recognition of a company's involvement in a

cyber-information-sharing arrangement can engender greater confidence from both its customer base and its existing and potential partners. Countless mergers and acquisitions transactions have failed because of poor cyber policies, *see* Seth Berman & Stroz Friedberg, *Cyber Security: The weakest link in M&A transactions*, Fin. Director (Apr. 22, 2014), http://tinyurl.com/okfjy6l, and cyber events such as last year's massive Target breach have highlighted very publicly that that a company is only as secure as its vendors. Target's systems were breached through security credentials that Target provided to an air conditioning service company. For similar reasons, information-sharing across supply chains is also critical. (Cyber Playbook, *supra*, at 56 n.148.)

For all of its benefits, cyber-information-sharing is not without its costs. This is particularly so for private companies, and largely stems from the fact that information-sharing works best when tailored among similarly situated organizations. Sharing information with a peer, rather than a stranger, means that less is lost in translation and efficiency is thus increased. The problem, however, is that the peers of private companies are often their competitors. Sharing valuable cyber-threat information is, at first glance, understandably counterintuitive. The truth, however, is that a rising tide really does raise all ships in the context of cybersecurity.

But the basic notion of benefiting a competitor is not all that is at play. Disclosing information to a cyber-network inevitably means that the information is no longer within a company's control. This runs the risk that such information may be used for other than its intended purpose. For example, information regarding a certain vulnerability may find itself outside of the network and in the public domain. The result could be its exploitation by potential threat actors, a loss of confidence by customers or partners, and potential regulatory fines for failure to comply with various cyber best practices. There also exists the risk of inadvertent disclosure *within* the network. Companies who unintentionally include their trade secrets or the personally identifiable information (PII) of their employees or customers may be handing their competitors an unintended boon.

Antitrust Enforcement Policy on Collaborations

Even if an industry surmounts these obstacles and agrees to share their cyber information, there is still one more hurdle to jump: antitrust. The ABA's Standing Committee on Law and National Security is one of many organizations that have commented on the antitrust concerns with respect to this information-sharing, stating that "antitrust concerns have triggered suspicion about close coordination among corporate competitors, including discussions of cybersecurity information sharing." (Cyber Playbook, *supra*, at 59.) The committee further noted that it would be appropriate for companies collaborating on cybersecurity information-sharing to address antitrust concerns, but also highlighted that both prior DOJ guidance and discussions with former Antitrust Division attorneys support the notion that antitrust is not a roadblock to properly conducted cyber-related information-sharing.

In response to these antitrust concerns stemming from competitors' collaborations on cybersecurity, the DOJ and the Federal Trade Commission (FTC) issued on April 10, 2014, an "Antitrust Policy Statement on Sharing of Cybersecurity Information" [hereinafter Cybersecurity Antitrust Statement], *available at* http://tinyurl.com/mqnwldy. This joint policy statement provides American industries with the clarity they need to share their cybersecurity information without violating the antitrust laws that the DOJ and FTC enforce. The agencies noted that "properly designed sharing of cybersecurity threat information is not likely to raise antitrust concerns" and can "help secure our nation's networks of information and resources." (*Id.* at 1, 6.) Recognizing the benefits of cyber collaboration, the agencies made clear that they "do not believe that antitrust is—or should be—a roadblock to legitimate cybersecurity information sharing." (*Id.* at 1.) The agencies' primary statement of their antitrust enforcement intentions is that information for collaborative cybersecurity efforts should not contain "competitively sensitive information—such as recent, current, and future prices, cost data, or output levels." (*Id.* at 4.) 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. The agencies provided examples of types of information that would typically be benign: malware signature detections, identified IP addresses, or target portals of known denial of service attacks. In most instances, these kinds of information would not contain anything competitively sensitive that would have a material effect on the prices charged by or the amount of output of the companies engaged in the collaborative cybersecurity effort, even if the companies were direct competitors.

In many ways, the Cybersecurity Antitrust Statement affirms enforcement policies regarding information-sharing that the two federal antitrust agencies have articulated numerous times. In 2000, the DOJ specifically referenced collaborative infrastructure security efforts among competing electrical power generation companies in a business review letter issued to the Electric Power Research Institute (EPRI), a nonprofit organization committed to providing and disseminating science and technology-based solutions to problems facing the energy industry. (Letter from Joel I. Klein, Assistant Attorney Gen., Antitrust Div., to Barbara Greenspan, Assoc. Gen. Counsel, EPRI (Oct. 2, 2000), http://tinyurl.com/pm5lyww.) EPRI had sought a statement regarding the DOJ's antitrust enforcement intentions with respect to EPRI's proposed information exchange. The proposed information exchange was designed to reduce security risks in the energy industries—risks that were attributed to increased dependence on computers and interconnectivity by market participants and their supply chains. The Antitrust Division determined that the proposed exchange of best practices and information related to cybersecurity vulnerabilities would not restrict competition in any of the energy-related markets. Such an information exchange would be limited to only physical and cybersecurity issues and, importantly, would exclude discussions on company-specific competitively sensitive information, such as price, purchasing, and future product innovations.

Perhaps in anticipation of the joint statement, the DOJ explained just months beforehand that, while the antitrust 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." (Renata B. Hesse, Deputy Assistant Attorney Gen. for Criminal & Civil Operations, Antitrust Division, Remarks at the Conference on Competition and IP Policy in High-Technology Industries: At the Intersection of Antitrust & High-Tech: Opportunities for Constructive Engagement 10–11 (Jan. 22, 2014), http://tinyurl.com/k4tm55n.)

The two federal antitrust agencies have published and revised multiple versions of a joint "Antitrust Guidelines for Collaborations among Competitors," commonly called the "Antitrust Joint Venture Guidelines"—most recently in April 2000. The Antitrust Joint Venture Guidelines indicate that if a competitors' joint venture has a primary procompetitive purpose and does not contain potential anticompetitive harms that outweigh the benefits, the federal antitrust agencies commonly will not challenge the competitors' joint venture. The Cybersecurity Antitrust Statement applies the analysis structure stated in the Antitrust Joint Venture Guidelines and concludes that cybersecurity collaborations among competitors that do not involve the exchange of competitively sensitive information are unlikely to raise any antitrust concerns.

That the DOJ and FTC made the effort to reaffirm in a joint statement—a relatively rare event in federal antitrust enforcement—this long-standing policy is one more example of how the federal government is, without legislation, encouraging greater cybersecurity in the private sector. That move largely began early last year when President Obama signed Executive Order 13636 on "Improving Critical Infrastructure Cybersecurity." (78 Fed. Reg. 11,739 (Feb. 19, 2013).) While the order is more commonly known for its direction to develop voluntary standards aimed at private sector use, it also highlighted the critical need for private entities to share cybersecurity information in order to secure the nation's IT infrastructure. The Cybersecurity Antitrust Statement will further that goal.

Next Steps for Cybersecurity Collaboration

Encouragingly, many industries have already created their own corporate sharing groups that provide both legal and effective opportunities to identify and protect against vulnerabilities in their networks. The most common of these industry groups are information sharing and analysis centers (ISACs). (Cyber Playbook, *supra*, at 57 n.152.) ISACs generally function as technical information clearinghouses for various industries. For example, the communications, electric, emergency response, and national health industries all have their own ISACs. (*See Member ISACs*, Nat'l Council of ISACs, www.isaccouncil.org/memberisacs.html (last visited Aug. 23, 2014).) Their services can include risk mitigation, incident response, and prompt alerting across an industry, all with the goal of providing their users with accurate, actionable, and relevant information. Not only do they share this information among themselves, but they may also inform other sectors and government bodies.

Although all strive to the same goal of protecting their industry members and thus the nation at large, different ISACs have different levels of maturity and efficacy. The Financial Services ISAC (FS-ISAC) is often regarded as the paramount of both. It provides timely and accurate threat information by communicating with its members multiple times per day. (Fin. Servs. Info. Sharing & Analysis Ctr., https://www.fsisac.com (last visited Aug. 23, 2014); *see* Cyber Playbook, *supra*, at 58 n.154.) The FS-ISAC is effective, in part, because of the principles underlying its operation. Its formal operating rules are deliberately designed to mitigate the sharing of sensitive corporate information with competitors. 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 requests. As such, the FS-ISAC is an example of an information-sharing system that works to the benefit of its members while accounting for the bounds of US antitrust laws.

The utility of the FS-ISAC was readily apparent in 2012 when the financial sector was bombarded with a series of distributed denial of service attacks that attempted to cripple their online services. The FS-ISAC functioned as a sounding board for its members to discuss response strategies. It even facilitated necessary cooperation with other industries such as Internet service providers. (Cyber Playbook, *supra*, at 58.) As specific industries like the financial sector become more frequent targets of cyber-attacks, their ISACs are playing a larger and exceedingly more important role in recognizing and responding to those attacks.

Other industries are beginning to take advantage of the lessons learned through the FS-ISAC. Partly in response to recent data breaches involving popular retailers such as Target and Neiman Marcus, the retail industry has announced its development of a retail ISAC. (*See* Retail Cyber Intelligence Sharing Ctr., http://tinyurl.com/nns3v5p (last visited Aug. 23, 2014).) Significantly, the development of the Retail Cyber Intelligence Sharing Center (R-CISC) will be in close coordination with the FS-ISAC. It is part of a greater effort by the two industries to work together regarding cybersecurity issues. Sandy Kennedy, the president of the Retail Industry Leaders Association, 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." (*Retailers Launch Comprehensive Cyber Intelligence Sharing Center*, RILA (May 14, 2014), http://tinyurl.com/pr6gppe.) 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.

Armed with greater clarity about the relative risks and merits of cyber-information-sharing, established and developing industries should strive in the future to achieve the level of integration, success, and legality attained by the FS-ISAC. The R-CISC is an encouraging step in that process.

Ultimately, the decision to participate in an information-sharing network will be a strategic one, based on both the benefits and the risks. Thanks in part to the DOJ's and FTC's recent joint guidance, antitrust concerns are less likely to be one of those risks. ■