New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
SEPTEMBER 7, 2021

Spies Like Us: Why Every Company Needs To Worry About Corporate Espionage

Recent SEC actions in the cybersecurity context suggest that corporate espionage may pose not only a competitive challenge for publicly traded companies, but also a complex disclosure issue. Companies must be mindful of not only how they guard their precious data from enemies within, but also how they publicly talk about those measures.

BY SIDHARDHA 'SID' KAMARAJU

"Espionage" conjures up images of spies slinking through dark alleys, cozying up to potential targets at luxurious parties, and trading a country's most guarded secrets. Company executives know, however, that espionage is a threat in the corporate world as well. So-called "corporate espionage"—or the theft of company data by a company insider—can cost companies their competitive advantage and deprive them of millions of dollars in profits. Insider breaches occur in all industries—whenever a company has valuable data, from product designs to personal customer data to proprietary technology or methods, that company is a potential target of corporate espionage. Now, further complicating the issue, recent SEC actions in the cybersecurity context suggest that corporate espionage may pose not only a competitive challenge for publicly traded companies, but also a complex disclosure issue. Increasingly, companies must be mindful of not only how they guard their precious data from enemies within, but also how they publicly talk about those measures.

The Increasing Threat of Corporate Espionage

In 1789, Samuel Slater may have become America's first corporate spy. That year, Slater emigrated from England, and brought with him closely guarded secrets about British techniques for manufacturing cotton that would revolutionize the American textile industry. In the centuries since, however, corporate espionage has become a scourge rather than a boon for many American companies. Congress has tried to address the problem through legislation by enacting, among other statutes, the Economic Espionage Act and the Defend Trade Secrets Act. Despite these legislative efforts, however, companies in every sector continue to grapple with the harm caused by corporate espionage. For example, in 1997, the year after Congress passed the Economic Espionage Act, the FBI arrested, among others, employees at Bristol-Meyers Squibb, Gillette, Kodak and Avery Dennison for the theft of millions of dollars' worth of trade secrets.

SIDHARDHA 'SID' KAMARAJU

Recent DOJ action also shows that the problem remains very much alive. For example, in April of this year, federal prosecutors convicted Dr. Xiaorong You, a former Coca-Cola employee, of stealing trade secrets from her former employer to start her own competing company. Dr. You retained Coca-Cola documents on her computer after signing a written agreement in which she falsely represented that she had cleared her computer of the documents, and then photographed the documents with her phone while they were on her computer screen to bypass Coca-Cola's security measures. Those documents included trade secrets reportedly valued at $120 million. Dr. You used those trade secrets to start

her own company in China, which received millions of dollars in funding from the Chinese government.

While the *You* case is a striking example of the corporate espionage threat, it is not an isolated one. For example, recently the DOJ convicted (1) a scientist at a U.S. petroleum company who stole $1 billion worth of trade secrets; (2) a former employee at a U.S. aviation company for stealing tens of thousands of files about a developmental aircraft radar system from the company's computer networks; (3) a foreign businessman for conspiring with an engineer at a major U.S. manufacturing company to steal information about semiconductor equipment; (4) a scientist for stealing medical research from a U.S. hospital; (5) a former director of a U.S. pharmaceutical company, for stealing, among other things, research protocols and drug compound data; and (6) a former employee of a U.S. oil and gas company for stealing information about proprietary technology used by the company. These cases demonstrate that—despite the threat of criminal penalties—greed will continue to drive some corporate insiders to try to victimize their employers by stealing trade secrets.

Moreover, corporate espionage is often not a matter of solely personal greed, but also of state action. The U.S. government has repeatedly detailed efforts by foreign governments to steal valuable data from American companies, whether through hacking into their computer networks from outside, or compromising those networks from within. Indeed, the problem has reached such significant proportions that, according to FBI Director Christopher Wray, in 2020 the FBI was working on "1,000 investigations involving China's attempted theft of U.S.-based technology, in all 56 of [the FBI's] field offices, spanning almost every industry and sector."

Increased law enforcement focus on the problem is of course a welcome development. But at the same time, law enforcement efforts are not a cure-all for American companies. For one thing, given the significant corporate espionage cases that occurred within just the past few years, it is apparent that potential prison time may not be enough to deter a company insider determined to profit illegally from a company's confidential information. Furthermore, if a company insider does steal trade secrets, there is no guarantee that the company would discover that breach and be able to alert law enforcement. And finally, law enforcement investigations into insider threat cases can present complicated and disruptive issues for a company—the very systems that a company spent considerable resources trying to keep private could very well be subject to public scrutiny in a criminal investigation and any subsequent prosecution.

The SEC's Statements About Corporate Espionage and Public Reporting

It's not just the FBI that has focused on the corporate espionage problem, but the SEC as well. In 2014, the SEC adopted Regulation SCI, which requires certain market participants to adopt policies to ensure the integrity of their computer systems, and to report "system intrusions," including by insiders, to the SEC. Five years later, in December 2019, the SEC released its "CF Disclosure Guidance: Topic No. 8" about "intellectual property and technology risks that may occur when [companies] engage in international operations." In this guidance, the SEC's Division of Corporate Finance specifically highlighted the "risk of theft of technology, data and intellectual property" through "corporate espionage, including with the assistance of insiders." Significantly, the December 2019 guidance also described the connection between corporate espionage and a public company's disclosure obligations, indicating that a company may need to make disclosures when corporate espionage impacted a company's "business, including [its] financial condition and results of operations, and any effects on [its] reputation, stock price and long-term value." Finally, the SEC instructed companies to consider whether they had "adequate controls and procedures" in place to prevent corporate espionage, including to detect "unauthorized intrusions into commercial computer networks" and "other forms of theft and cyber-theft of your technology and intellectual property." Taken together, Regulation SCI and the 2019 guidance send a clear message that the SEC expects public companies to implement protocols to prevent corporate espionage and to consider the risk of an insider breach when making public disclosures.

Recent SEC enforcement actions indicate the potential pitfalls for a company that doesn't take these issues seriously. In June 2021, the SEC fined First American Financial Corporation, a real estate settlement services company, almost half a million dollars in connection with the company's disclosures about its cybersecurity protocols and vulnerabilities. In *First American*, a vulnerability in the company's computer systems resulted in more than 800 million files containing customers' personal information being inadvertently posted online. The company filed a public disclosure about the leak, but the SEC deemed it insufficient because, before making the disclosure, the company's executives had not learned of a separate system

vulnerability. As a result, in the agency's view, the company's disclosures about the vulnerability of its system and the "magnitude of risk" to the company's information were incomplete and thus deficient.

First American is just the latest SEC enforcement action based on inadequate cybersecurity protocols and disclosures. In 2019, the Operations Clearing Corporation was required to pay a $15 million civil fine for, among other things, violating Regulation SCI by failing to secure its computer systems. Then, in May of this year, the SEC fined GWFS Equities, Inc., a registered broker-dealer, $1.5 million for GWFS's failure to file SARs and filing deficient SARs about cyberattacks that failed to include specific information about the perpetrators and methods involved in the attacks. Taken together, *First American*, *GWFS* and *Operations Clearing* demonstrate some of the perils of a company faced with a cybersecurity incident—the company must ensure that it has a complete picture of the points where its systems may be compromised, and if there is a breach, be prepared to disclose the "who, what, when, where, and why" of the breach.

An insider breach can present these same issues—just as with an external cyberattack, a bad actor has compromised a company's data, calling into question the company's data protections and protocols and the continued value of its proprietary information. Given Regulation SCI, the SEC's 2019 guidance, and the *First American*, *GWFS* and *Operations Clearing* actions, the SEC likely would adopt a similar approach to insider threats as cyberattacks, scrutinizing a company's insider threat policies and public reporting after a material corporate espionage incident. In fact, one of the failings that the SEC highlighted in *Operations Clearing* was the fact that the company did not have a policy of inventorying all network devices, which is a typical risk factor when judging an organization's safeguards against insider threats. Given the ever-escalating pace of corporate espionage, companies are going to have to quickly come to grips with the SEC's approach to these issues.

Getting Ahead of the Problem

So what's a company to do? Luckily, there are steps that a company can take proactively to mitigate insider threat issues.

First, companies need to ensure that they have robust policies and practices in place to detect and prevent corporate espionage in the first place. Any company that relies on sensitive proprietary data should examine its current protocols to address insider threats with the help of experienced counsel. Although each company needs to think about its unique business and where the threats exist, at a bare minimum in-house counsel should ask themselves these questions:

- Do our screening procedures at hiring turn up red flags, like financial irregularities or unexplained foreign travel?
- Do our network controls restrict access to sensitive information to only those employees who truly need it to do their jobs?
- Do our systems allow us to tell what's happening on our network in real-time, such as through real-time auditing?
- Do our practices allow us to accurately inventory computer equipment with access to our proprietary data, including, for example, portable hard drives or other removable storage media?
- Do we maintain our proprietary data in such a way as to ensure that the data would receive trade secret protection under statutory and common law?
- Do we have security protocols in place so that we can detect unusual behavior, like unexplained wealth, or properly act on employee tips?
- Do our employment agreements sufficiently protect us if an employee does try to capitalize on stolen trade secrets?
- Does our reporting structure ensure that the executives who are responsible for public disclosures have access to a complete picture of the company's vulnerability to an insider threat?

Experienced counsel can help with issues that may come up when answering these questions, including employee privacy issues, data protection, whistleblower programs and cybersecurity policies. Thinking proactively about these issues can help companies breathe a little easier.

Second, if a company is victimized by corporate espionage, the company should consult with counsel about how to respond. For example, counsel can help the company coordinate with law enforcement agencies, working to protect the company's interests during the investigation and any subsequent prosecutions. Moreover, counsel can help to ensure that the company's public disclosures about the incident do not further compound the issue by drawing regulators' scrutiny. Managing the response to a corporate espionage incident is a critical component of minimizing the already substantial headache caused by an insider breach.

Sidhardha 'Sid' Kamaraju *is a partner in Pryor Cashman's white-collar defense + investigations, financial institutions, and litigation groups.*