FBI and MI5 Sound Alarm on Covert Chinese State Interference in Private Sector

July 26, 2022 J. Nicholas Bunch, Kit Addleman, Kenneth Parker

PRACTICES Intellectual Property Litigation, Privacy and Cybersecurity, China, Trade Secret Litigation

Federal Bureau of Investigation ("FBI") Director Christopher Wray and Security Service ("MI5") Director General Ken McCallum issued a joint warning to business and academic leaders in London this month, "sending the clearest signal yet about the risks posed by Chinese state action" to U.S. and UK companies' trade secrets. Their joint session highlighted the Chinese Communist Party's ambitions to overtake the West by 2050 in key sectors, including technology, advanced research, and product development. The Directors explained that where the Chinese government senses it cannot accomplish this feat, it has successfully misappropriated the trade secrets of private companies and universities through espionage, tech transfers, cyberattacks, and simple flattery. Citing the widely reported hacking of Microsoft Exchange Server software last spring and ample other examples, Director Wray explained, "The Chinese government is set on stealing your technology," "using it to undercut your business and dominate your market," while "using every tool at their disposal to do it." The Directors Wray and McCallum identified some of the tools that they attribute to Chinese government's effort:

- **Intelligence Officers.** The Chinese government has used people unaffiliated with the Chinese Communist Party to assist in recruiting and gathering information to steal trade secrets. One example given by the directors was that of a British aviation expert who was recruited online, offered ostensibly legitimate employment, and was then asked and paid to provide technical information on military aircraft. It was later determined that the company was run by Chinese intelligence officers.
- **Hacking.** The directors explained that Chinese state-sponsored hackers have become increasingly adept at bypassing network defenses. The hackers "monitor network defender accounts and then modify their campaign as needed to remain undetected," blending into what appears to be normal activity.
- **Hidden Investments and Partnerships.** The directors also highlighted the use of shell companies including some SPACs to exert control over what appears to be an unaffiliated company and precludes data that would reveal Chinese state ownership during due diligence.
- **Legislation.** The directors also argued that various Chinese laws weaken foreign corporations' defenses against intellectual property and trade secret theft. For example, recent enactments require companies deemed as "critical infrastructure" to store their data in China, obligate Chinese employees in China to assist Chinese intelligence operations, and punish companies operating in China that implement international sanctions. The directors explained that some of these laws even facilitate hacking efforts, such as the government-sanctioned tax software, which U.S. companies have discovered is a conduit for malware delivery.

But these tactics are no reason for a savvy company to avoid doing business in or with China. A company well-equipped with an appreciation for the threats posed, the right tools, and a team of experts can manage risks the Chinese government's devices pose to its proprietary information. The directors recommend the following:

- **Coordination with Agencies.** The directors encourage coordination with FBI and MI5, offering to work alongside companies and share on the front-end "everything from details about how Chinese government hackers are operating to what they're targeting." When an incident occurs, Wray promises assistance to degrade the threat.
- **Strategic Planning.** Deputy General McCallum recommends regular discussions internally and with the Board around these threats, security culture, identification of the company's "crown jewels"—key competitive advantages and trade secrets which would compromise the company's future if stolen, and controls to assess risks with respect to funding and partnerships.

Properly assessing the threats foreign interference, from any source, poses to a company is crucial to protecting its trade secrets and competitive edge. Director Wray has previously stated that economic espionage cases with a link to China increased by approximately 1,300 percent over the past decade, and a new case is opened every 10 hours. Building the right team to advise the company on the front-end and acting quickly when the specter of interference arises assists with shoring up defenses to these known threats. Haynes Boone has both a deep and wide bench of attorneys who can assist with the myriad issues arising from this threat.

As the FBI and MI5 have reiterated in their joint statement, Chinese state interference in US and UK businesses is prevalent, and can be perilous for companies without a plan. Awareness and preparation with counsel can provide the prophylactic businesses need to protect against and respond to this ever-increasing threat.