April 28, 2023

Recent DOJ Prosecutions Underscore the Risk From "Insider" Cyber Threats

On April 17, 2023, the U.S. Attorney's Office for the Eastern District of New York ("EDNY") announced two separate complaints alleging that operatives of the People's Republic of China ("PRC") used U.S. technology companies to advance PRC strategic objectives, including through the use of a PRC-based employee of one such U.S. technology company. According to one complaint, the PRC-based employee acted at the direction of the PRC government to use his access to the company's internal systems to identify the accounts of pro-democracy activists and interfere with videoconferences hosted on the company's platforms by a prominent Chinese dissident residing in New York City.[1] The employee identified in the complaint was thus able to use his position within the company to exploit back-end controls over the company's products and advance PRC policies.

The EDNY complaints follow another prosecution related to an insider threat, the April 14 Department of Justice ("DOJ") indictment of Airman Jack Texeira, a member of the U.S. Air National Guard accused of unlawfully transmitting classified U.S. defense information.[2] The DOJ alleged that Texeira used his "Top Secret" security clearance to access and exfiltrate confidential documents pertaining to U.S. defense strategy, including American policy and projections regarding the ongoing conflict in Ukraine.[3] The Pentagon has characterized the leak as posing a "very serious" risk to U.S. national security.[4]

Together, these prosecutions highlight the potential threats posed by so-called insiders to U.S. public and private sector organizations.

Key Takeaways

- **The private sector should be proactive in identifying and countering insider threats**. Cyber incidents associated with insider threat actors are likely to remain a source of economic loss and potential liability for the private sector. As such, companies should take active measures to limit their exposure to such threats, and to mitigate the harm that such insiders can cause. Steps that companies can take include improving coordination between IT security and human resources to identify and mitigate the risk of potential insider threats, proactive monitoring using behavioral analytics to identify anomalous insider activity, and training employees to identify any potential insider threats and properly safeguard data from both internal and

1 *Eight Chinese Government Officials Charged with Directing Employee of a U.S. Telecommunications Company to Remove Chinese Dissidents from Company's Platform*, Department of Justice (April 17, 2023), available here. The second EDNY complaint did not allege direct action by company insiders, instead describing how agents of the PRC's 912 Special Project Working Group (the "Group"), part of the Ministry of Public Security, created thousands of online personae on U.S. social media networks to disseminate pro-PRC and anti-democracy content. The DOJ announcement of that complaint is available here.

2 *United States* v. *Teixeria*, Case No. 1:23-04293, Compl. at 1 (D. Mass Apr. 14, 2023).

3 *Id.* at 3, 5.

4 *Leaked documents a 'very serious' risk to security: Pentagon*, AP News (April 10, 2023), available here.

external threats. Such insider threat programs must, however, also account for competing concerns about employee privacy and protection.

- **Insider threat actors in both the private and public sector raise national security concerns**. The DOJ's increased focus on the risks to national security posed by insiders at public and private sector organizations means that a broad set of companies are likely to be the subject of increased scrutiny when it comes to such threats.[5] For example, companies that contract with government may be subject to heightened regulatory scrutiny of how the companies vet employees and protect against unauthorized data exfiltration.

- **Fighting cyber threats with an "all tools" approach continues to be a focus for U.S. law enforcement**. The DOJ's criminal indictments against individuals responsible for the insider attacks against private and governmental organizations are representative of the "all tools" approach described by Deputy Attorney General Lisa Monaco in her July 2022 keynote address at the International Conference on Cyber Security.[6] The DOJ's use of the courts to interdict threat actors constitutes an important prong of the strategy, alongside efforts by the Department of Defense, the Intelligence Community and other government organizations.

We will continue to provide updates on developments in cyber threats.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Peter Carey
+1-202-223-7485
pcarey@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Associate Neil Chitrao contributed to this Client Memorandum.

[5] The Department of Defense has implemented its own Insider Threat program through the Defense Counterintelligence and Security Agency. That program includes personnel vetting, training, and network monitoring. In the wake of the prosecution of Airman Texeira, the Department of Defense and other governmental organizations are likely to enhance the measures they have in place to counter insider threats. Information regarding the Department of Defense's insider threat program is available here.

[6] *Deputy Attorney General Lisa O. Monaco Delivers Keynote Address at International Conference on Cyber Security (ICCS 2022)*, Department of Justice (July 19, 2022), available here.