LJN LAW JOURNAL NEWSLETTERS

Cybersecurity LAW & STRATEGY®

An ALM Publication

January 2019

# What the U.S.' Pursuit of Foreign Nation-State Hackers Means for Cybercrime Victims and Targets

**By Ronald Cheng and Mallory Jensen**

For years, the U.S. has maintained an active enforcement campaign against overseas cyber criminals, with prosecutors charging hackers who have engaged in schemes including phishing, credit card fraud and identity theft. While these past efforts have not been haphazard, they have not necessarily been part of a specific drive to address the serious issue of foreign cybercrime committed by nation states. Recent announcements by the Department of Justice (DOJ) show that this enforcement campaign is accelerating and expanding.

At the beginning of November 2018, the U.S. Attorney General announced DOJ's "**China Initiative**." The initiative is based on findings that "Chinese sponsorship of hacking into American businesses and commercial networks has been taking place for more than a decade and is a serious problem that burdens American commerce." Its goals are to "identify priority Chinese trade theft cases, ensure that we have enough resources dedicated to them, and make sure that we bring them to an appropriate conclusion quickly and effectively." In the months preceding the announcement, DOJ announced an escalating series of indictments against foreign defendants, particularly individuals from China and Russia.

For example, DOJ recently brought charges against Chinese and Taiwanese companies and their executives for stealing semiconductor industry trade secrets; indicted Chinese officials accused of hacking into computers to steal sensitive commercial technological, aviation and aerospace data; and charged Russian intelligence agents with waging an extensive spear-phishing campaign to install malware that would collect passwords and enable them to access sensitive material. Other DOJ charges show that cyber crime covers more than the trade secret offenses that make up a substantial part of the China Initiative: DOJ recently indicted Russian GRU officers for computer hacking, wire fraud, aggravated identity theft and money laundering related to their efforts to undermine and retaliate against the investigation of widespread doping by Russian athletes.

As U.S. law enforcement continues to address the efforts of foreign state-sponsored actors to target U.S. companies' assets, it is timely to review what companies need to know about the factual and legal parameters of these cases, as well as how they should prepare themselves both to prevent such attacks on themselves, and what to do in the event of such an attack.

## Criminal Hacking Conduct and Legal Theories

Criminal charges against foreign individuals who have allegedly hacked or otherwise harmed U.S. companies involve an appreciable number of hacks that have been executed by elite teams of hackers working within

**Ronald Cheng** is a partner and **Mallory Jensen** is counsel in O'Melveny's White Collar Defense & Corporate Investigations practice.

government or military units dedicated to hacking and stealing information from politicians and companies in other countries. The teams' methods vary depending on the target and purpose of hacking, but the hacker teams are often alleged to play a long game of familiarizing themselves with targets, infiltrating them either through hacking their systems or by becoming employees or trusted collaborators with them to obtain trade secrets or other coveted inside knowledge or documents.

For instance, in ***U.S. v. Dokuchaev***, a team of Russian hackers carefully reconnoitered an Internet company's network after gaining unauthorized access and spent the next two years extracting user information and eventually defrauding users. One of the hackers was extradited to the U.S. from Canada and sentenced to prison after a guilty plea.

In ***U.S. v. Yu Pingan***, the defendant pleaded guilty to installing malware on companies' systems that allowed them later to obtain account and other information from the companies.

And in ***U.S. v. Wang Dong***, a group of hackers within China's People's Liberation Army were charged with hacking computers over the course of eight years to obtain information from steel, specialty metals, nuclear power plant, and solar companies in the U.S. that would be useful to Chinese competitors. Although it has not been possible to extradite these hackers (there is no U.S.-China extradition treaty) or otherwise bring them to face charges, the indictments led to a U.S.-China agreement that neither side would "conduct or knowingly support cyber-enabled theft of intellectual property." In addition, more recent cases have focused on trade secret theft involving computer crime and so-called "human source" compromises.

DOJ often prosecutes such cases under the **Computer Fraud and Abuse Act (CFAA)**, which prohibits knowing or intentional access to a "protected computer," (*i.e.*, one belonging to a financial institution, the federal government, or that is used in or affecting interstate or foreign commerce or communication), to gain access to restricted information, as well as any transmission of code that damages protected computers. Courts have not hesitated to apply the law extraterritorially, as long as the affected data is based in the U.S. On the other hand, certain courts have held the CFAA may not apply when an employee accesses an employer's system, as opposed to an outsider or former employee doing so.

Depending on the scheme used, prosecutors may also bring wire fraud and trade secret theft charges. When theft of trade secrets to benefit a foreign government is involved, charges may be brought under the **Economic Espionage Act**. Charges have also been brought for being a foreign agent (18 U.S.C. §951) or under the **Foreign Agents Registration Act (FARA)**, which requires such agents to publicly disclose their relationship with another country if they are acting in any political or quasi-political capacity in the U.S.

In general, the computer crime charges require either that the defendant accessed data in the U.S., or that the defendant used instrumentalities, such as email accounts, based in the U.S. Given the foreign nature of these prosecutions, there is also the fundamental issue of how to hale the defendant into court. Formal extradition applies only when the U.S. has an extradition treaty or agreement with the defendant's country; otherwise, investigators may try to lure or otherwise remove a defendant from the country of residence to one where the defendant can be detained for extradition or expulsion. Effecting service on foreign corporations has also been a challenge, although recent amendments to the Federal Rules of Criminal Procedure may make it easier for prosecutors to serve process on a company or organizational defendant without coordinating with a foreign government. Beyond these challenges in pursuing foreign hackers and actually bringing them to the U.S., the U.S. government in some cases has gone so far as to

impose sanctions related to persistent cybercrime.

## Practical Considerations

Companies aware of all these cases should continue to assess what they can do to protect themselves, and what to do if and when they are targeted by hackers or other thieves of trade secrets. In general, recommended protection measures are not that different from general cybersecurity practices. As the Federal Trade Commission (FTC) has explained in its "**Start With Security**" guidance, companies can take a number of measures to reduce their exposure, beginning with not collecting and storing personal information they don't need, whether of customers or employees.

Access restrictions may help, both as to limiting who may see data and requiring strong passwords and authentication, as well as strong encryption methods, network segmentation and secure methods of remote access to the company's network.

Companies must also be careful when retaining vendors to ensure that they adhere to a high level of security and update their security procedures to keep defenses current. Companies that take such measures can reduce the risk of falling victim to hacking of any kind. Nevertheless, hackers will still try to gain access to prized targets through social engineering, and training can help employees serve as another line of defense in the company's security plan. But if companies make it more difficult for hackers to enter their networks or compromise their employees, the hackers may turn their attention elsewhere.

When a hack or other intrusion does happen, companies must consider their options for requesting help from law enforcement. DOJ recently revised its guidance for companies that decide to report hacks directly to criminal authorities. In "**Best Practices for Victim Response and Reporting of Cyber Incidents**," DOJ explains that companies considering reporting a hack should preserve log files to assist in post-incident analysis, as well as recording any ongoing suspicious activity.

DOJ recommends that if a company believes the incident may have been criminal in nature (*i.e.*, rather than just an innocent employee mistake), it should contact law enforcement as soon as practicable, without fear that a federal investigation will cause additional disruption. DOJ also notes that the **Cybersecurity Information Sharing Act (CISA)**, a 2015 law, makes cooperation with law enforcement simpler by authorizing private entities to share cyber threat information with the authorities. For example, CISA includes certain liability protections when companies share cyber threat indicators and defensive measures with law enforcement.

Companies whose trade secrets have been stolen must consider additional factors when reporting to law enforcement. First, victim companies will want to continue to protect their trade secrets, despite the breach, and while federal law authorizes a court to enter a protective order to preserve confidentiality, victims should consider the defense's access to protected material to prepare a defense. Second, any criminal case brought by the government could result in a stay in any civil case brought by the victim company, which could delay civil relief for the company.

## Analysis

Many U.S. companies have a wealth of information, whether in employee and customer databases, trade secrets, or both, and they will always be targets for this kind of foreign espionage. Guarding against those threats and remedying the consequences of an attack is not easy, but understanding these fact patterns, as well as how the government prosecutes such crimes, can help companies to prepare.

—❖—

Reprinted with permission from the January 2019 edition of the LAW JOURNAL NEWSLETTERS. © 2019 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877.257.3382 or reprints@alm.com. # 081-01-19-03