June 4, 2019
KEYNOTE REMARKS AS PREPARED FOR DELIVERY
NCSC Director William Evanina
International Legal Technology Association (ILTA)
LegalSEC Summit 2019
(Note: These prepared remarks may differ from the remarks delivered)

Thanks for inviting me to speak today. Great opportunity.

I understand you had an exercise yesterday focused on cyber incident response. I want to start today by emphasizing the importance of this activity.

All firms should have a strategy and policy in place for incident response. Every employee should be educated on the plan. The plan should be exercised at least twice year and tested in a tabletop exercise. The strategy and policy should also include personnel from across the enterprise – not just your CISSO, CSO, and CIO, but your general counsel, acquisition, procurement, and human resources leaders.

As this audience already knows, law firms both large and small are increasingly being targeted by cyber actors, including nation-state intelligence services. You are among the most prized and lucrative targets for cyberattacks.

Why? You're a one-stop shop for hackers, whether they're criminals, hacktivists or foreign spies. You keep intellectual property, sensitive mergers and acquisition details, and confidential personal data on many clients. Targeting you is an efficient way to access data on many organizations, instead of targeting each directly.

The bottom line is you have been or soon will be targets of cyberattacks because you have information valuable to foreign governments, hacktivists, criminals, and others.

A key foundation of the legal profession is the duty to protect client information. Data breaches are a major liability threat, professional responsibility threat, and reputational threat facing you.

So how do cyber threats to law firms intersect with my world -- the counterintelligence world -- which focuses mostly on threats from nation states?

Every day, we see advanced cyber operations from China, Russia, Iran, and North Korea targeting the U.S. Many of these efforts are focused on economic espionage.

More than ever before, adversaries are stealing America's information, innovation, technology, and research and development. The private sector has become the new geopolitical battlespace. It's an asymmetric warfare where nation states are targeting companies in nearly every U.S. sector, costing our nation jobs and an estimated $300 to $500 billion per year.

These companies are your clients. Their data is in your hands. Hackers are targeting your firms to get at that data. And you have a fiduciary duty to those clients.

China Threat

No country poses a greater counterintelligence threat than China. As the FBI Director recently noted, China has pioneered a societal approach to stealing innovation any way it can.

President Xi Jinping seeks to position China as the world's geopolitical, military, and economic superpower. To get there, China is pillaging nearly every sector in the U.S, including Artificial Intelligence (AI), robotics, Information Technology (IT), energy, and aerospace.

The FBI has noted it has economic espionage investigations that lead back to China in nearly all of its 56 field offices. Roughly 90 percent of the Justice Department's economic espionage cases from 2011-2018 involved China.

To get at our innovation, China is using an array of lawful and unlawful techniques including foreign investment, corporate acquisitions, as well as cyber intrusions and supply chain threats.

An example: today is the 30th anniversary of the Tiananmen Square massacre, a topic taboo in China. Chinese internet firms are now using the latest AI and machine learning tools to block content on the massacre from appearing online in China. China pumped an estimated $1.3 billion in venture capital into America's AI companies from 2010 to 2017. I suspect some of that AI knowledge is now being used to help erase Tiananmen Square from the web in China.

The actors involved in such efforts include Chinese intelligence, state-owned enterprises, ostensibly private companies, graduate students and researchers, and others working for China.

You should also be aware of the laws in China that compel every Chinese citizen and company to assist in national security or intelligence work. This should concern you if represent clients that work in or with China.

Article 7 of China's National Intelligence Law states, "Any organization or citizen shall support, assist, and cooperate with state intelligence work in accordance with the law, and maintain the secrecy of all knowledge of state intelligence work."

Article 28 of China's Cybersecurity Law states, "Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."

Article 11 of China's National Security Law states, "All citizens of the People's Republic of China …. shall have the responsibility and obligation to maintain national security."

What does this mean for you? If you're doing business in China or representing clients there, you will likely be a target. If you handle Committee on Foreign Investment in the U.S. (CFIUS) work related to China, you will be likely a target. If you handle clients in key tech sectors or handle mergers and acquisitions involving China, you will likely be a target.

In December, APT-10 hackers tied to China's spy service were indicted for hacking into managed service providers (MSP) to get access to the clients of these MSPs around the world. One of APT-10's victims, according to a recent private cybersecurity report, was a law firm that works in high-tech IP and helps Chinese companies enter the U.S. market.

In 2016, three Chinese hackers were indicted in New York for targeting several law firms to steal inside information about pending mergers and acquisition deals and trade on it. The unlawful gains exceeded $4 million.

We've seen this activity dating back to 2012, when a D.C. law firm was targeted by Chinese hackers as it represented a client in a trade dispute with China.

China isn't the only nation-state actor to worry about. Russia is an extremely a potent cyber operator and Iran is also posing a growing cyber threat.

In the 2017 *NotPetya* attack, Russian military hackers implanted destructive malware in a program in Ukraine that spread and destroyed computer networks around the globe. One collateral victim was a major law firm that was paralyzed for weeks. The firm's IT team put in 15,000 hours of overtime to recover and had to wipe its system clean. The firm was denied a multimillion-dollar insurance claim related to the attack.

Last year, nine Iranians were indicted for a massive cyber theft campaign on behalf of the Iranian government that targeted research and intellectual property at 320 universities in 22 countries. At least 47 companies -- and a law firm -- were also hacked.

Cyber Attack Methods

Phishing remains among the most common attack techniques, even for nation states. This is low cost / high reward. Some have estimated that more than 90 percent of cyber-attacks involve spear-phishing. It just takes one careless employee to click on a suspicious link and your entire system is compromised. How well is your firm protected?

In October 2018, two Chinese intelligence officers and eight others were indicted for hacking U.S. and European aerospace firms over five years to steal trade secrets on commercial aircraft engines. How did they get in? Spear-phishing.

Ransomware is obviously another major cyber threat to law firms, as are business e-mail compromise, insider trading schemes, and malicious insiders.

Supply chain attacks also pose a growing threat, not just to law firms, but to the entire private sector and government. Nation-state adversaries are increasingly infiltrating our trusted third-party suppliers and vendors to target the equipment, systems and information we use every day.

If, like most companies, your law firm uses third parties to store data or manage your IT, carefully vet those third parties and their security practices to protect yourself. That third party can pose a huge risk to you.

Your firm's position in the supply chain can also make you a target. Nation-state or criminal hackers may seek to infiltrate your firm as a stepping-stone to gain access to corporate clients and their information. As I said earlier, law firms are often just a vector for the adversaries to access client data, which is their ultimate target.

How can you avoid becoming the weakest link in the supply chain? In April we launched National Supply Chain Integrity Month to educate the private sector and government about supply chain risks. I encourage you to visit our supply chain risk management materials at NCSC.gov

While many threats to the legal sector still come from cyber criminals with a financial motive, my message to you is that nation states, particularly China, are likely to play a growing role in future cyber-attacks that will affect you and your firm.

Threat Mitigation

What can you do to protect yourself? Some of the basic steps include the following:

Identify, prioritize, and commit to protecting your crown jewels.

Know who you are doing business with. Vet your third-party vendors, understand their security practices, and set minimum security standards for them. Ask the right questions before procuring their products or services. Supply chain security can be expensive, but lack thereof is costlier and can result in pronounced, long-lasting damage.

Strengthen your cyber security and hygiene by protecting your credentials, by using dual factor authentication and by patching regularly. Beware of spear phishing: never click on suspicious links or attachments, particularly from unverified or unknown sources. On social media, maximize your social media privacy settings; use caution in what you post on social media; never accept friend requests from strangers; and validate friend requests through other sources. And when traveling abroad with your laptop or other electronic device, have no expectation of privacy.

You should also implement insider threat programs. The trusted insider with access is often the gravest threat to your organization.

As I noted earlier, it's critical that you institute a comprehensive, enterprise-wide security posture. Ensure these policies are socialized with every employee and practiced twice a year. Include Acquisition, Procurement, and Human Resources personnel in the security plans.

Finally, maintain enduring connectivity to the U.S. Government on current threat intelligence and security best practices. Enrolling in the FBI's InfraGard program is a great first step. You can also visit the "Know the Risk, Raise Your Shield" page at the NCSC website for tips on how to protect yourself.

Thank you.