FBI's Boston office warns businesses of venture capital scams

Lucia M. Ziobro and Vincent B. Lisi are both special agents in charge of the Boston division at the U.S. Department of Justice Federal Bureau of Investigation. Ziobro wrote an op-ed warning local businesses

about venture capitalist scams.

W. MARC BERNSAU | BUSINESS JOURN

By Lucia Ziobro
Apr 4, 2014

The FBI's Boston outpost is warning Boston-area businesses of scams involving malicious foreign venture capitalists. In its push to educate the private sector and raise awareness about economic espionage and cyber counterintelligence, the FBI released the following op-ed to the Boston Business Journal.

Community policing in a high tech world

The FBI recently released a notification to technology companies and research facilities, which include colleges and universities in the Boston area, warning them of the possible perils of entering into joint partnerships with foreign venture capital firms from Russia. The warning was based on the FBI's growing concern that the purported reasons offered by the Russian partners mask their true intentions. The FBI believes the true motives of the Russian partners, who are often funded by their government, is to gain access to classified, sensitive and emerging technology from the companies. The Boston area has among the nation's highest concentration of technology companies, many of which support the defense industry. The warning urged those contacted by Russian venture capitalists to remain vigilant and cognizant of the potential losses and compromises of company assets.

The warning is part of the FBI's growing alliance with the private sector. The FBI issues dozens of such bulletins every year to help businesses protect their intellectual property and systems from criminal threats. In the past, such information might have been provided to the private sector, but with limited details due to of the restrictions of sharing classified information. With the uptick of economic espionage and export control or "counterproliferation" cases prosecuted in federal courts, the FBI now has the ability to use unclassified and publicly available information to warn businesses and

entrepreneurs of the possible perils of partnering with foreign investors. With regard to Russia, the FBI offered this insight, “The offer may seem lucrative at first, but it could also mean the permanent loss of intellectual property rights and manipulation of dual-use technologies.”

Over the past decade, the FBI has increasingly shared detailed information with those in private industries in an effort to prevent and deter crimes and to prevent sensitive technology from being lost.The change was precipitated by law enforcement’s widely accepted belief that engaging the private sector through partnerships and by sharing information about the threats facing them is an effective way to prevent and detect threats. Since 9/11, the FBI advocates intelligence-led policing which aims to detect and deter crimes before they are committed by anticipating crime trends through sound analysis. The FBI combines this relatively new practice with the well-accepted community policing model that relies on enlisting community groups, non–profit agencies, private businesses and neighborhood residents to work together to defeat factors commonly associated with fostering crime. Understanding and predicting future threats rather than merely reacting to ones as they appear, while at the same time sharing information about those threats, is a more effective way to protect our national interests.

The FBI’s proactive stance is illustrated by the genesis of the warning about the Russians. When the FBI observed a new pattern of Russian government-funded businesses increasing their footprint in Boston and Silicon Valley by seeking joint ventures with U.S. companies and academic institutions, its analysts and agents reviewed the pattern to discern the factors and motivations behind their sudden emergence. It was determined that the partnerships were primarily promoted by the Skolkovo Foundation, founded by Russian president Dmitry Medvedev in 2010. The Foundation may be a means for the Russian government to access our nation’s sensitive or classified research, development facilities and dual-use technologies with military and commercial applications. This analysis is supported by reports coming out of Russia itself. The Foundation has been

reported to be a critical part of Medvedev's plan to modernize the Russian economy, decrease dependency on oil revenue, create a more diversified economy based on high-technology and innovation and to completely renovate its military technology equipment and arsenal by 2020. According to news reports, in the fall of 2013, the Foundation signed an agreement with the Russian vehicle manufacturer Ojsc Kamaz. Kamaz is also a Russian defense contractor who supplies the Russian military with armed and armored vehicles and was scheduled to produce more than 100 all terrain transports to the Russian strategic missile troops last year. The agreement enabled Kamaz to establish a research and development facility in the Skolkovo 'innovation city' located near Moscow. The FBI fears that Kamaz will provide Russia's military with innovative research obtained from the Foundation's U.S. partners.

The analysis raised another area of concern regarding the Foundation's history of corruption. The Foreign Corrupt Practices Act prohibits U.S. firms from engaging in corrupt actions overseas. In November 2013, the Russian Federation's Accounts Chamber fined over 200 managers and senior employees at the Skolkovo Foundation after an investigation of the Foundation's use of government funds. The fines followed criminal charges against the Foundation's executives for the misuse and embezzlement of $1.5 million through various schemes.It is the intent of the FBI for the recipients of the bulletin about Skolkovo to use the information to inform their decision making process when selecting foreign investors to protect their interests which results in safeguarding our nation's interests.

The FBI's effort to collaborate with industry dates to the mid-1990's. As it became clear criminals would increasingly exploit technology for illicit gains, the FBI initiated a pilot project called InfraGard, which was designed to engage those in the technology industry. The pilot began in the FBI Cleveland Division in 1996 as a way to create an exchange of information about cyber investigations with local information technology experts and academia. Sharing information about intrusions, trends and vulnerabilities with private

industry was seen as a way to help secure private computer networks and harnessing industry expertise. (The program proved so successful that it was replicated in each of the FBI's 56 field offices and later expanded to include terrorism, criminal and counterintelligence matters.) InfraGard is especially valuable in light of Director of National Intelligence James Clapper's recent prioritization of cybersecurity over that of both terrorism and espionage.

Building on the success of InfraGard, the FBI has initiated other partnerships. Under the FBI's Counterintelligence Strategic Partnership Program, agents work with defense contractors, firms that develop defense or export controlled products and universities that conduct sensitive research on the government's behalf. The threat from foreign governments is so prevalent that the FBI Boston Division, which covers one of the nation's most concentrated areas of technology firms and research universities, has two full-time employees for Strategic Partnership outreach. Their sole responsibility is to warn companies about the risks of foreign businesses and insiders or cyber hackers seeking to steal their proprietary products.

FBI Director Comey recently spoke at the RSA Cyber Security Conference and remarked about how important it was for the FBI to protect the private sector's proprietary information and customer data. "We must share as much information as we can, as quickly as possible, so that companies can minimize any breach. And we must continue to build strong relationships." Director Comey encouraged companies to use the FBI's malware database. If a company has been hacked, it can send the malware to the FBI and in most cases, receive a report within hours of how the malware works, what it might be targeting and whether others have suffered a similar attack. This information sharing assists the FBI in its investigations of high level, state sponsored intrusions into the private sector companies seeking proprietary information.

Though it may sound alarmist, losses of technology, research and intellectual property are a real danger. Preventing foreseeable and predictable losses is

critical to our nation. U.S. technology replicated overseas means U.S. employees may lose their jobs and U.S. investments may suffer losses. Furthermore, diverted technology could affect the primacy of the United States in both economic and military terms and it could compromise our nation's security. In the wrong hands, especially those of foreign governments, everyone loses except our adversaries.

Lucia Ziobro is assistant special agent in charge of the FBI's Boston office.