Tips welcome as FBI sleuths keep a finger on cyberthreats

Blake Sobczak, E&E reporter

Published: Tuesday, September 20, 2016

For the past two decades, the FBI has dispatched eyes and ears to conference rooms across the United States.

The agents aren't undercover; they're invited. And instead of meeting in a boardroom or in secret, almost anyone can listen in.

These FBI representatives are part of InfraGard, a widespread but seldomly publicized U.S. government-sponsored program to keep private-sector operators of critical infrastructure, such as ports and power plants, apprised of the latest threats to their systems.

"There's been some press that we're some sort of FBI secret thing, but we're not secret at all," said Kristina Tanasichuk, president of the National Capital Region chapter of InfraGard, which encompasses Virginia, parts of Maryland and Washington, D.C.

The InfraGard model relies heavily on private-sector input, with individual, not-for-profit chapters distributed around each of the nation's FBI field offices. At first, companies may be attracted by the promise of learning the FBI's thinking on matters ranging from computer viruses to active shooters. But in practice, the FBI representatives often take a back seat and let the companies share information and learn from one another, according to multiple InfraGard participants and organizers interviewed by *EnergyWire*.

Tanasichuk is CEO of the Government Technology & Services Coalition, a Virginia-based advocacy group for small security companies, when she's not volunteering her time with the FBI.

"InfraGard started before 9/11, but the real pressing demand for information sharing came after, because everyone said, 'Why didn't we put these pieces together?'" she said. "InfraGard tries to do that, so that the utility grid does not get attacked, and we stop that shooter from killing kids at the mall. That's the point of the program."

That casual approach is deliberate: InfraGard meetings are as much about sharing intelligence as they are about breaking the ice among people who normally keep a low profile but who would be first in line to respond to a cyber or physical strike on the nation's infrastructure.

FBI special agent Kara Sidener, who works as InfraGard coordinator for the National Capital Region chapter, said the emphasis on individual relationships sets the program apart from other quasi-governmental, information-sharing efforts. "Institutions don't normally trust institutions; people trust people. So by bringing it down to that individual level, sometimes a lot more can get done," she said.

Sidener pointed out that the vast majority of U.S. critical infrastructure, from the power grid to manufacturing plants, is controlled by the private sector. "In order for us to be effective at doing our job, we need to have strong partnerships with those owners and operators so that when bad things happen, it's not the first time that we're speaking," she said.

Each FBI field office assigns an agent to the local InfraGard chapter, with some, like Sidener, working full-time on outreach. She said most of InfraGard's new members hear about the program via word of mouth. Prospective members must sign a waiver to get access to a secure FBI portal, in addition to agreeing to undergo a basic "security risk assessment" to take part in all InfraGard has to offer.

Sidener said that in her experience, Edward Snowden's sweeping 2013 disclosures of domestic spying programs run by the National Security Agency haven't chilled participation in InfraGard, despite its open affiliation with the U.S. intelligence community.

"Folks that come into this program already get the importance of information sharing," she said. "Members are very willing to help us. ... Somebody's not going to volunteer to have the FBI do record checks on them if they don't want to help."

Cyber roots

InfraGard chapters are divided along the lines of the 16 federally designated critical infrastructure sectors, allowing for groups to meet and discuss specific vulnerabilities. Companies typically donate office space for periodic meetings, sometimes allowing sponsors to bring in coffee and refreshments.

Martin Kessler, director of new energy solutions for AES Corp. and energy sector lead for the National Capital Region's InfraGard chapter, said his company came to be involved in the FBI program "as an additional channel for sharing information and networking with both government and private sector peers responsible for protecting critical infrastructure."

He called public-private partnerships "an integral part" of AES's strategy for guarding its electric power assets amid a "constantly changing threat landscape." Joining InfraGard helped the company learn about the programs and capabilities of the FBI, Kessler explained in email, adding that the resources have since been incorporated into the utility's incident response plans.

Most InfraGard events and resources cover cybersecurity in some form, owing to the program's genesis as a way to support FBI cyber investigations out of the agency's Cleveland office. Once vetted, InfraGard members can tap into the FBI's Malware Investigator tool, which compares samples of suspicious code against hundreds of thousands of previous malware submissions.

The National Capital Region chapter, based as it is around D.C., often discusses cybersecurity for government facilities. Houston's InfraGard chapter has a huge oil and gas industry presence, while Idaho's is more concerned with threats to agriculture.

Minnesota's InfraGard chapter counts members from the utility, medical device and retail industries, among others.

Eran Kahana, who sits on the board of directors for the Minnesota chapter of InfraGard and serves as its general counsel, said the bulk of the group's activities are "weighted toward cyber."

"Everything can be attacked these days by cyber [means] — it's the easiest vector of attack, and one that we are definitely paying attention to," said Kahana, whose day job sees him advise companies on intellectual property and technology matters as counsel for the law firm Maslon LLP.

That's not to say other risks are off the table. Kahana pointed to a recent stabbing rampage at a mall in St. Cloud, Minn., in which an attacker with reported links to the Islamic State group injured nine people before being killed by an off-duty police officer. Past InfraGard meetings in the region have addressed homegrown violent extremism, "active shooter" scenarios and threats to landmark retail destinations like the Mall of America in Bloomington, Minn.

"You wouldn't think Minnesota would be attracting anything, but here we are finding ourselves in the forefront with [threats] related to terrorism and infrastructure security," he said.

Kahana cast InfraGard participation as a means for companies to show they're serious about managing risk and engaging in information sharing. But it cannot just be "a one-time thing," he cautioned; rather, "you need to do it systematically."

Threats and secrets

Parts of InfraGard are hidden from public view, a practice InfraGard's backers defend as necessary for an organization aimed at addressing weak spots in U.S. infrastructure.

An upcoming National Capital Region Members Alliance talk on lessons from the utility industry's GridEx III exercise, which pitted grid operators against simulated hackers, drones and physical attackers, is closed to the press. GridEx took place in a private but unclassified setting last year.

Privacy advocates have raised skepticism about what, from the outside, can appear to be little more than a huge web of FBI tipsters. The program's secrecy has also drawn unwelcome attention from hackers and conspiracy theorists who paint InfraGard's true purpose in apocalyptic terms.

In 2011, InfraGard's Atlanta chapter saw its website defaced and its members' sensitive personal information spilled online following an attack by hackers affiliated with the LulzSec group.

Hector Monsegur, one of the hackers responsible for that episode, said he had not been familiar with InfraGard beforehand but rather targeted the FBI-affiliated organization as "low-hanging fruit."

He now says he regrets that decision, among others that ultimately landed him in FBI custody. He has since switched sides and now works as a security researcher, helping companies find and patch their cyber vulnerabilities.

The 2011 hack "led directly to my arrest, actually," he told *EnergyWire* in a Twitter message, noting that the FBI is "very proactive when it comes down to InfraGard."

A more prosaic challenge for InfraGard chapters stems from their members who may lack security clearances to interact with FBI at all levels.

The FBI's partners run up against some of the same information-sharing barriers that other public-private partnerships at the Department of Homeland Security have faced.

"Who to share, what to share, with whom? ... Those questions are still a bit vexing to the community," said Tanasichuk of the InfraGard National Capital Region Members Alliance. "You don't want information getting into the wrong hands, [but] you want the people who need to know to know as soon as possible."

At public InfraGard webinars and meetings, it's not unusual for the thorniest questions from the audience to go unanswered. During a recent teleconference addressing the threat from "ransomware" — malicious software that encrypts user data and holds the key hostage — the speakers declined to identify victims by name in a public forum.

Tanasichuk, who is wrapping up the first year of her three-year tenure as chapter president, said she has steered the group to focus on grid physical and cybersecurity, hosting briefings on a Dec. 23, 2015, cyberattack on Ukraine's power distribution network that left hundreds of thousands of that country's citizens without electricity.

"Critical infrastructure owners and operators, they stay up at night; they're on the cutting edge" with cybersecurity, she said, adding that generally, "I don't think people understand the impact [cyber] can have on the country."

E&E PUBLISHING, LLC
www.eenews.net

E&E Publishing, LLC
122 C St. NW, Ste. 722, Wash., D.C. 20001
Phone: 202-628-6500 Fax: 202-737-5299
www.eenews.net