SECURITY
SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

What to Expect When Working with Cyber Cops

What your company, as a victim of a computer intrusion, should expect when working with the Feds.

By Steven Chabinsky
December 1, 2013

In last month's column, we explored the *Top Five Reasons to Report Computer Intrusions to Law Enforcement*. This month's column will provide you with a sense of what your company, as a victim of a computer intrusion, should expect when working with the Feds.

Who's At the Door?

Within the United States, the FBI and the Secret Service are the primary agencies for investigating computer intrusions. Of the two, the FBI is the lead if the matter involves cyber spies or cyber terrorists. Both the FBI and the Secret Service work with state, local and international law enforcement, as well as with industry partners, providing the added benefit of a global, coordinated response. The Special Agents working on a cyber squad are super smart, and they typically have a degree in computer science or network administration and earned the same professional certifications as your IT staff. These men and women easily could be working for higher pay in the private sector (and many already have), but instead they have chosen to serve their country. Simply put, they deserve your respect, and I have no doubt they also will earn it. When they show up at your door, you can expect them to look, well, like Feds. But that doesn't have to be the case. It is perfectly acceptable to discuss your company's dress code with them before they arrive, in order to have them better blend in. It also is a good idea to get to know the FBI and the Secret Service in advance of a problem.

Will They Help Fix Our Computers?

Shoring up your network defenses (similar to helping you lock your doors and windows, or setting up your alarm system) is not the primary role of law enforcement. Catching the bad guys is. Said differently, the Feds are seeking to spend less time with you, and more time hunting the adversary through cyberspace. Although the FBI and Secret Service often share information that will help mitigate your problem (such as the type of malware used or the method of intrusion), you should not expect them to focus on updating and patching your systems or recommending new products. You must employ or retain

your own computer security and incident response team for that purpose. The FBI and Secret Service want to work with your team, benefit from their knowledge, answer your questions and then move on to identifying and stopping the threat actor.

What Will They Want?

First, law enforcement will want to ensure that you do not tip off the intruder. Doing otherwise could cause the attacker to become hostile, destroy logs and create additional backdoors to harm you later. In furtherance of operational security requirements, you may be asked to limit your discussions about the intrusion, to avoid using your internal email to communicate about the intrusion, and to take advantage of a law enforcement request to delay statutory data breach notifications. Second, law enforcement will want to preserve and collect evidence. They will not want you to turn off your computers since that will result in the loss of volatile memory, but disconnecting briefly from the Internet may be okay. They will ask for technical data, to include network- and host-based incident logs and up-to-date network topology maps. Third, law enforcement will want to get a better sense of potential insider and external threats to your organization. They might ask you about disgruntled current and former employees, in addition to the ability of well-meaning, unsuspecting employees to have used infected thumb drives, clicked bad website links, or opened spoofed emails. Fourth, law enforcement might want your direct investigative assistance. This could include your voluntary use of government technologies that can help protect you while identifying the attacker. You may even be asked to engage in email or phone communications with the attacker.

When Will It End?

Computer intrusion investigations can be quite complex. Law enforcement may work on-site for two to four weeks. Once they leave, they will continue their investigation to find the perpetrators. Doing so could take months, as they chase down IP addresses, coordinate action overseas and seek court process against subjects and co-conspirators. Just because they aren't calling you with new information doesn't mean they aren't still working and making progress. Similarly, just because they are working and making progress doesn't mean they should be calling you. Although law enforcement likely will notify you during the investigation if they discover additional tactics or targeting aimed against your company, they are not inclined to reveal detailed information about their subjects and may be under legal restrictions not to disclose it.

How Does It End?

Your chances for success are highest when you combine your company's internal vulnerability mitigation and detection efforts with meaningful law enforcement coordination to stop the attack at its source. When it comes to security, nothing beats an FBI or Secret Service phone call saying, "Good news. We arrested them, and your information is safe." At that point, when the Feds say, "We couldn't have done it without your help," you'll say, "Right back at you… and thanks."

About the Columnist:

Steven Chabinsky is General Counsel and Chief Risk Officer for cybersecurity technology innovator CrowdStrike, which provides incident response services, cyber intelligence feeds, and a next generation, big data platform for continuous threat detection, attribution, and prevention. He previously served as Deputy Assistant Director of the FBI's Cyber Division.