SECURITY
SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

Top 5 Reasons to Report Computer Intrusions to Law Enforcement

Text

Even when not legally required, reporting cyber crime to law enforcement can act as a deterrent for other malicious actors contemplating future attacks.

By Steven Chabinsky
November 5, 2013

Judging by today's headlines, it is only a matter of time until every company – yours included – is going to experience a computer intrusion, or perhaps another computer intrusion. When that happens, you may find yourself working with law enforcement. Sometimes, they will be the ones calling you. A recent survey shows that just less than 10 percent of all data breaches are first identified to the victim by law enforcement. At other times, it quite literally will be your call, both in terms of judgment and in picking up the phone.

There are a number of very good reasons to report crime even when doing so is not legally required, and cybercrime is no exception. First, catching the bad guys is the surest way to get them out of your system, to deter others who might consider your company an easy mark, and to satisfy a civic responsibility to protect others from similar attacks. With this goal in mind, it is clear that law enforcement has authorities that companies do not have and never will have. The most important of these is the ability to make arrests. Yes, it's true that there was a time when cyber criminals were seldom caught, but today's coordinated law enforcement is increasingly effective at locating cyber thieves both at home and abroad. As reflected at www.cybercrime.gov, a Department of Justice website, the good guys are chalking up a lot of wins. In one press release, you can read how the FBI, together with NASA's Office of the Inspector General, the Estonian Police, private industry and not-for-profit groups, all worked together to locate and arrest six individuals in Estonia who conducted an Internet fraud scheme that infected more than four million computers.

In another case, the U.S. Secret Service was called upon when a hacker in Hungary broke into a major hotel chain's network, stole confidential information and then threatened to make everything public unless he was given a job. The feds gave him a plane ticket to Virginia, an employment interview and, you'll like this part, a two and a half year jail sentence. Significantly, the hacker never got the chance to make good on his threat to release the company's stolen information. This example demonstrates the second good reason for reporting to law enforcement. Catching the bad guys can result in the complete recovery of a victim's data or otherwise minimize the harm of an intrusion. It simply is not the case that once data is stolen it is always replicated, dispersed and released. Law enforcement very well may be able to get an otherwise out-of-control situation under control. It is good messaging to state that your company cooperated fully with law enforcement when it learned of a breach precisely because, in doing so, your

company is demonstrating that it took every meaningful step to remedy a serious situation.

Third, working with law enforcement is more likely to helpfully inform your internal security efforts than to waylay them. This is especially true if, prior to contacting law enforcement, your company already has begun its incident response efforts with a competent internal team or an expert cybersecurity forensic services firm. The FBI and the Secret Service, for example, are trained to work with members of your team and consultants, not against them. Although law enforcement is not situated to give a company advice on how to patch its software or configure its networks, the government may be in a position to provide your company with information about the methods, capabilities and intentions of the intruder in ways that can feed directly into your security plan and response options. For example, companies find it valuable to learn when they are being targeted for foreign sponsored espionage rather than by a run-of-the-mill criminal. When China's military is the culprit, changing everyone's password will not suffice.

Fourth, to the extent an intrusion results in the loss of customer personally identifiable information, it may trigger state data breach notification requirements, to include a duty to notify law enforcement. Regardless, it is helpful to know that most, if not all, state data breach laws permit companies to delay notification to accommodate a law enforcement request. Although consumers may expect immediate notification, law enforcement is in a better position to know whether publicly revealing an intrusion is likely to cause more harm than good in light of continuing vulnerabilities of the victim or a bad guy who remains at large. Having the ability to delay reporting based on a justified law enforcement request may prove invaluable during times of crisis.

Fifth, reporting cybercrime provides government agencies with the data necessary to follow trends and calculate the impact of this growing problem. Accurate crime data, in turn, is useful to ensure proper funding to address the issue in ways that lower your risk. Reporting also is a data source that feeds into government warnings and alerts about evolving criminal tactics and the effectiveness of industry best practices to thwart them. In contrast, leaving law enforcement uninformed, untrained and underfunded is a surefire way to exacerbate this problem.

Still, if you end up working with law enforcement, you should know what you are getting into. In next month's column, I will explore law enforcement's investigative approach to cybercrime, describing what you should expect when you're expecting them.

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 intrusion detection, attribution, and prevention platform. He previously served as Deputy Assistant Director of the FBI's Cyber Division.