The Truth About Cyber Threat Information Sharing

This article was originally published on Fox Business on November 5, 2014.

by Brian E. Finch

Brian E. Finch
Public Policy
+1.202.663.8062
brian.finch@pillsburylaw.com

Brian E. Finch is a partner in Pillsbury's Public Policy practice in Washington, DC. He is a recognized authority on global security matters and is co-leader of the firm's Global Security practice.

Everywhere you turn, someone is calling for increased cyber threat information sharing: Congressional members, former Congressional members, former Executive branch officials, learned experts, my Aunt Selma (but not Patty).

Enough. I'm sick of hearing about it.

I know—information sharing is valuable. I get it. The government has lots of information on cyber threats that the private sector could find useful, and vice versa. So trust me, I'm no information sharing-hater.

What I am sick of, however, is the notion that information sharing is the key component in the fight against cyberattacks.

Nope. Not true.

Information sharing is just a very basic step. Frankly, given the trends in cyberattacks, the value of information sharing is actually decreasing, relatively speaking.

So, as always with cybersecurity, a strong dose of reality and some fresh perspectives are needed.

Let's first start with the presumption underlying information sharing. Specifically, the tools and tactics used by cyberattackers will be used repeatedly, so sharing information will be critical to stopping most cyberattacks.

The definition of "Cyber Threat Indicator" set forth in the leading information sharing bill, the "Cybersecurity Information Sharing Act of 2014", echoes that theme. The indicators to be shared include:

- Malicious reconnaissance, cyber command and control;
- Methods for defeating a security control or exploitation of a security vulnerability
- Actual security vulnerabilities, including methods that allow attackers to exploit authorized users of systems; and
- The actual or potential harm caused by an incident.

That's actually a nice, expansive definition that could prove helpful to companies.

Still, I have several fundamental problems with the idea that information sharing is absolutely critical and we need to give the Executive branch authority to implement it.

My first problem is that that information ignores Finch's Law:

"Cyber defenses cannot keep pace with the increasing sophistication or creativity of cyber-attacks."

The attackers are incredibly motivated, skilled, and have every incentive to find ways around existing defenses. As a result, we always seem to be a step or two behind when it comes to our defenses.

Consider for instance that cyberattackers have lapped us by negating the whole idea of "signature-based" defenses. Signature-based defenses, as some of you may know, are defenses that rely on spotting code or other embedded information linked to known malware. If a malicious signature is spotted, it is then blocked.

There are two problems with that approach: a) cyberattackers figured out long ago how to create malware with signatures that constantly morph, thereby evading signature-based

defenses, and b) according to my friends at FireEye/Mandiant, at least 70% of malware is now used only once.

Well then, there goes one critical justification for information sharing: The information shared may not actually be useful.

Also, let's be honest here, government-based information sharing is not going to be quick, much less delivered in real time. That's especially true given all of the inevitable privacy hurdles that will have to be cleared first.

So, even if one contends information sharing is vital, I would argue in favor of using industry-based solutions that operate in real time. I'm aware of several non-signature-based technologies that use behavioral analytics to find malware. Once a threat is found, those same tools develop threat indicators and automatically share them with other devices.

My biggest gripe about the information sharing obsession is this: It distracts us from the fact that the government is basically doing NOTHING material that will slow down or stop cyberattacks.

Brian, how dare you!

Look, I've written about this before. To use military parlance, hackers have complete freedom of movement. They proceed with little to no interference from security officials, and have all of the time they need to study their targets and practice their attacks so they can strike at their leisure.

That is why the new director of the National Security Agency, Adm. Michael Rogers, said that one of the biggest cybersecurity challenges is that "people don't pay a price for attacks." The information sharing obsession aggravates me then because it obscures what we really need to do: Attack the cyberattackers.

I am talking about the U.S. government (not the private sector) performing one of its fundamental, constitutionally-assigned obligations: Protect America from enemies foreign and domestic.

For heaven's sake, the criminals are plundering our national treasure like we were an unarmed Spanish galleon laden with gold. Simultaneously, foreign governments walk into our information systems, steal secrets and plant malware with amazing success.

I hate that. It offends me.

I'm offended because "information sharing mania" blinds us to the need to inflict pain on the attackers so they think twice about committing misdeeds.

So what needs to happen? First, Washington must make it clear to every nation that our digital borders are as sacred as our physical borders. Attempts to breach them will be considered an affront to our sovereignty. Without such an explicit cyber policy, our enemies will never think twice about launching cyberattacks.

Next, Washington has to take real steps to inflict pain on cyberattackers. This includes more aggressive law enforcement that will result in bringing hackers here to America to face justice under our laws and judicial system.

The actions of foreign governments also need to be addressed. The President and Congress have to act forcefully—which includes imposing economic sanctions and disruption of foreign assistance and diplomatic ties on countries that are known cyber offenders. And, in very limited circumstances, it could also mean the use of force.

Look, at the end of the day I support information sharing. Battlefield intelligence is always vital. But for heaven's sake, let's be realistic about what has to happen. We can't sit back and just try to hold our ground.

We need to make the enemy understand that if they throw a punch, something really nasty will come right back at them.

Share that opinion with your congressman please.