Rethinking Cyber Defense

This article was originally published on *Fox Business.com* on June 20, 2014.

by Brian E. Finch

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

Brian E. Finch is a partner in Pillsbury's Washington, DC office. His practice focuses on counseling on regulatory and government affairs issues involving the Department of Homeland Security, Congress, the Department of Defense, and other federal agencies.

We are not winning the cyber war.

There, I said it.

It isn't that we are necessarily "losing" the cyber war, but we definitely are not gaining ground on our adversaries. No material impact is being made on the volume of cyberattacks. In fact, recent estimates indicate that 97% plus of companies have suffered some form of serious cyber intrusion, and that it takes on average anywhere between 7 and 8 months to discover that an attack has occurred.

It is not as if the cost to conduct cyberattacks is rising, either. One can find any number of reports detailing how cybercrime is essentially a risk-free activity, as there is little to no chance that perpetrators will be caught or punished.

In many ways, it is a bleak picture. As I have written before, the math is completely wrong here. The cost of conducting attacks is far too cheap, and the mountain of money being spent on cyber defense is making only a slight impact on the tsunami of successful attacks.

The thing is, it's only going to get worse. Companies and governments rely too much on outdated models of cyber defense such as "signature" based defenses. Meanwhile, it is becoming so easy to create new malware that cyberattacks often use a piece of malicious code only one time so as to not set off current alarms.

So where does that leave us? Do we need Kryptonite to use against hackers? No, I believe it is time for a revolution in cyber warfare. Our cybersecurity model seems to only consider defense, focusing on ways to stop attacks or cleaning them up quickly. This "supply-side" approach just won't work – the incentives for conducting attacks are just too attractive for criminals to pass up.

Part of that is due to what I am going to refer to as "Finch's Law" of cybersecurity (very modest, I know). We are all familiar with "Moore's Law", which essentially sets forth the principle that computing power will double roughly every two years. Well, in the cyber context, the sophistication of attackers and malware doubles much more rapidly than that. Indeed it is only a matter of months, if not less, before cyberattackers can create new techniques to evade newly created defenses.

That evolutionary cycle has to somehow be disrupted.

But how can that be accomplished? In my humble opinion, I believe strong actions in both the public and private sector will be needed to alter the action/reaction model of cyber combat. More importantly, we need to stop thinking only in terms

of reaction. The paradigm must shift into a disruptive model, one that denies cyberattackers the luxury of safe rear areas and the unlimited ability to pick the time and place of battle.

Here, in particular order, are my thoughts on the components of the cyber revolution:

Government needs to step up: Too often we play a game of "blame the cyber victim". If someone suffers a successful cyberattack, well obviously they were lax or negligent in some way that contributed to the success of the attack. Bullfeathers, I say. Politicians and the public alike have to understand that sometimes cyberattacks will succeed despite the measures taken to defend against them. More importantly, government needs to be more aggressive in its offensive actions against cyber-attackers. I am not talking about "name and shame" tactics or federal indictments that will never result in a real prosecution. I am talking about real steps that will inflict pain on cyberattackers. This includes more aggressive law enforcement and a willingness to step on international toes to nab hackers residing in foreign jurisdictions. Most importantly, treat cyberattacks undertaken or encouraged by nation-states for what they are: a breach of our sovereignty and a national security matter. We would not tolerate repeated physical theft of goods or sabotage of our infrastructure by foreign agents, would we? No. We would respond with official actions such as sanctions. In certain cases, national security elements would retaliate. In other words, if it is time for the federal government to start inflicting some pain on our adversaries.

Create a negative feedback loop: It tears me apart to say this, but there does, on occasion, need to be consequences for companies that are lax in implementing cybersecurity measures. Not every successful attack means someone failed and should be punished, but there are times when clearly a company did not undertake sufficient measures to protect itself and its assets. In those cases, I'm sorry to say punitive measures may be called for, including litigation. I am very uncomfortable with this idea because I can see this spinning out of control rapidly – visions of "The Price Is Right" commercial breaks featuring ads screaming "Consumer alert! If you have been hacked, you need a lawyer! Call 1-800-I've-been-hacked and we will fight for your digital rights!" are dancing in my head. Unfortunately though, in the absence of companies stepping up and "properly" defending themselves, justice may have to play out in civil courts. I am also presuming here that such litigation will have beneficial outcomes like establishing basic "standards of care" for cyber defense, safe harbors that companies can use to defeat such litigation, and even the creation of an implied duty to disclose successful attacks even when no statute or regulation calls for such disclosure. Part of the challenge is that some companies are willing to stick their head in the sand when it comes to finding cyber threats. Well, maybe we need the courts to say "Fine, stick your head in the sand. Remember though you can still be shot in the tuchus."

Security as an autonomic function: Part of the problem we encounter in confronting cyberattacks is that, frankly, we think about defending ourselves. What I mean by that is that cyber defense is often approached as "Oh yeah, we should build in security too." We cannot afford to operate that way anymore. Cybersecurity has to be unconscious, automatic, and reflexive action that is innate. When we are born, we don't have to teach ourselves how to breathe or blink. Similarly, eons of evolution have given us a "fight or flight" reflex that takes over in a dangerous situation. Cybersecurity has to be the same way – it is automatically something we do, something that is ingrained in our DNA. By that, I mean when products or networks are designed, or when we make a decision to buy a product or use a service, security is a core consideration – one that is just as important as form, functionality, and price. Security cannot, and should not, simply be an "aftermarket" product, nor can it be something that you have to deliberately have to search for as part of the purchasing process. Buyers and sellers alike need to understand that because anything and everything can be penetrated in a cyberattack, cybersecurity must be a core component of every electronic device or information technology. The reality is that our adversaries are endlessly creative when it comes to penetrating systems, and our job is to make their task harder. Reflexively incorporating cybersecurity into

every technology and business decision will go a long way to raising the cost of conducting cyberattacks.

My point in all this is that there is too much focus on defense, and not enough of disrupting the paradigm that has led us to being constantly on our digital heels. Given the atmospherics surrounding conducting cyberattacks (they are cheap yet sophisticated, endlessly evolving, and often have the resources of a nation-state behind them), if we stick to fighting a defensive battle, we will lose the cyber war. Our enemies won't wear themselves down – no, we will slowly erode into defeat.

What is needed is to recapture the initiative. It is time to break out of our rigid way of thinking and go outside the box. It reminds me of Marshal Ferdinand Foch's (alleged) immortal declaration during the First Battle of the Marne:

"My center is yielding. My right is retreating. Situation excellent. I am attacking."

Let's take control of the cyber battlefield. It is time to feel pain and inflict it, uncover problems, and disrupt the enemy's freedom of movement. Without aggressive action, we will never regain control.

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | +1.877.323.4171

Pillsbury Winthrop Shaw Pittman LLP