Cyber Neologisms Likely Headed for the Dictionary

This article was originally published on Fox Business on November 21, 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.

I am fascinated by the idea of creating new words out of thin air. It is an interesting concept that slang such as "selfie" and "ginormous" can officially become part of the English language.

Given that, I have come up with some new words (and phrases) to try and capture some of what is going on in the world of cybersecurity. With that, in no particular order, I give you my official list of cyber neologisms:

Finch's Law

This is my take on Moore's Law, which points out the pace at which technology advances. After speaking with true cyber experts and doing some thinking about the problem, I came up with the following rule of thumb: Cyber defenses cannot keep pace with the increasing sophistication or creativity of cyberattacks.

That is a nice, pithy way of saying that we are always going to be a few steps behind the cunning of cyberattackers. Let's face it, they make lots of money off cyberattacks and can rest assured that the likelihood of being caught is extremely small.

So, cyber-criminals will continually develop new ways to penetrate systems, and the defenders will always be a step or two behind simply due to the inability to anticipate every type of attack.

In-law problem

First off, no, this is not a commentary on my personal life. It is a handy way to illustrate a complex problem, namely that when you acquire/partner with/or tie into another business, you get the bad with the good.

Think of it like the Vacation movies. Clark Griswold hit the wife jackpot with the lovely Ellen. A big problem Clark had, though, was that he now had to deal with the likes of Cousin Eddie, and lots of (hilarious) problems ensued.

Cybersecurity is not that different.

When you buy or team with another company, fantastic synergies can happen. The challenge is that you also inherit their problems – chief among them are information systems riddled with malware and weaknesses. Thus, businesses would do well to conduct thorough due diligence on the cybersecurity posture of potential partners.

Cyber beauty pageant

This is an interesting and disturbingly common phenomenon, one where companies measure their cybersecurity readiness not through a comprehensive risk-based analysis and audit, but rather by how shiny their toys are.

This is a dangerous proposition because it creates a sense of security under the theory that if we purchase the latest and greatest technology, we will be as safe as possible. While there is value in buying new toys, they will do you no good if they are not tied to a strategy that constantly evaluates the threat environment and adjusts defenses and response resources accordingly.

The digital ostrich

The 21st Century equivalent of "If I don't know about it, it isn't a problem." The theory goes that if you don't know about the breach or ongoing attack, you do not have to disclose it, much less worry about its consequences.

As I have noted before, the interesting thing about sticking your head in the sand is that the rest of your body is still exposed and can be easily hit. Nowhere is this more accurate than in cybersecurity. Attacks happen all the time, and the failure to even try to discover them will only have disastrous outcome.

Cyberattackers can linger for years, siphoning data in real-time. That kind of loss cannot be ignored, in part because, in all likelihood, the company has a legal obligation to be aware of cyber threats and take reasonable action to mitigate them.

Snowdentification

Ah, Mr. Snowden. His betrayal of secrets has had an impact on American foreign policy and national security that hasn't been seen since the Rosenbergs gave away the atomic bomb to the Soviets.

Anyway, "Snowdentification" is the jumbled process that causes concern over privacy to bleed into cybersecurity issues. This is a serious problem because in reality, privacy in the cyber defense context is of little to no concern.

The information being gathered and used to help cyber defenses has almost no personal information involved; rather it involves technically examining traffic to see if aberrant behavior (meaning malware) is present.

Yet, because the privacy debate has become so hot, thanks to Snowden, such reality is ignored when it comes to cyber defenses. Instead, people automatically assume government run cyber defenses create privacy problems.

Until Snowdentification is cleared up, we are all worse off.

Breach Bums

Breach bums are a curious lot. They are obsessively paranoid about the possibility of a successful cyberattack, and if one occurs their automatic response is that somehow the victim is to blame.

I find that position bizarre.

There are not many other situations where a person or company is the victim of a crime committed by sophisticated gangs or even foreign countries and people think "Boy, that company must have been negligent to allow that to have happened."

This is yet another reality warp field, one that completely ignores the fact that so many attacks are done using technology and methods that circumvent just about any defense available. I am at a loss as to why so many "Breach Bums" obsess over the possibility of cyberattacks, and yet are prone to blaming the victim.

I think that perspective is fundamentally unfair and is generally the result of a lack of understanding of how bad the cyber problem has become. If people knew how hard defending against cyber threats has become, they would not automatically assume the victim failed in some way.

Obsessive Compulsive Information Sharing Disorder

This is one of my favorite topics.

The notion that if government and industry sat down and just talked out their problems – namely sharing information about what cyberattacks look like – we can make huge progress in stopping future attacks. Again, I think information sharing has significant value and should be encouraged, but it is foolish to think it is THE answer – far from it.

Too many new cyber tactics are in use and, more importantly, used one time. It is because of that that information sharing is of increasingly limited value. Plus, obsessing over information sharing distracts from the need for a true strategic shift to the offense.

Government needs to step up and get cyber criminals and nation states on the run. Right now cyber criminals can pick the time, place, and method of attack. If all we are doing is trying to figure out when the attack is going to happen, we will lose.

The attackers have to be disrupted in order to actually slow down attacks and that won't happen by obsessively worrying about zeroes and ones being shared between government and the private sector.

One last good one I have heard, and must attribute to National Security Agency Director Admiral Mike Rogers, is "cyber blur".

According to Admiral Rogers, cyber blur is the notion that network defense is a responsibility that is an ad hoc, ill-formed responsibility for the public sector and private sector. Admiral Rogers refers to it as the "ultimate team sport" because no single sector has the total answer. It also refers to enemies combining resources, blurring tasks and creating partnerships that make attribution more difficult.

Whether you like the summaries or not, I am confident the above list reflects important ongoing issues and trends in cybersecurity. Feel free to use them as you see fit.

ATTORNEY ADVERTISING. Results depend on a number of factors unique to each matter. Prior results do not guarantee a similar outcome.

Pillsbury Winthrop Shaw Pittman LLP