Why Cybersecurity Must Be Defined By Process, Not Tech

This article was originally published in the *Wall Street Journal's* CIO Journal on December 11, 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.

As cyber-attackers grow more sophisticated, the best and most realistic cyber defense strategy for CIOs is process-based.

Perhaps the most challenging question associated with cybersecurity is determining whether "enough" security has been implemented. For CIOs, risk managers, directors and officers, this is no abstract question. The inability to get cybersecurity "right" will certainly lead to losses, including possible job losses.

Many try to boil this down to a few simple questions, namely what security tools should be bought and how much money should be spent in total on cyber security. These are simple, clean questions which one would think will lead to a better state of cyber preparedness.

They won't.

Those questions presume that there is some sort of cyber-alchemy formula, through which companies can determine with great accuracy the cyber tools and total dollar spend needed in order to dramatically increase security.

It would be nice if that were the case, but just like it would be nice to find a way to turn lead into gold, it is a flight of fancy that is destined to fail. Let me explain why.

First, there is no such thing as a cyber silver bullet when it comes to defensive technologies or services. The cyber threat constantly morphs thanks to highly motivated and skilled attackers, and, cyber criminals are smart enough to act like water: they follow the path of least resistance.

What about a cyber ecurity strategy focused on budget size? CIOs will welcome more budget dollars, especially as their superiors realize that threats are not just from "viruses", but also come from insiders, fake parts, and assorted other directions.

Unfortunately there is no good rule of thumb of what that budget should look like. Every business is different, and some will be more consistent targets of cyberattacks than others. Moreover, even if one could say "X" percent of the information technology budget should be spent on cybersecurity, there is no guarantee that the money will be spent wisely.

That leaves us then with a process-based model. A popular formula to use here is a "risk-based" strategy,

which in this case means risk equals threat plus vulnerability plus consequences.

Okay, so let's briefly examine the risk-based analysis components to get a sense of what needs to be examined and how it all fits together.

Let's start with the threat. In this case, I'm not talking about malware or denial of service attacks, but threat actors and their capability to cause harm. It is a simple, but effective analysis. Certain threats (meaning ones from nation-states and groups that have access to tools on par with those used by countries) simply cannot be stopped. If they cannot be stopped, don't waste too much time and money on trying to stop them.

There are also threats you could stop, but may well not be able to. This category includes organized crime and groups that operate with the knowledge and occasional support of governments. Those groups often use very sophisticated tools that can defeat almost any defense, but they also regularly use tools and software that companies can stop with advanced defenses and smart threat monitoring.

Finally, there are threats you should be able to stop. These are generally attacks launched by individuals or relatively amateur criminal gangs. Those groups tend to use "off the shelf" attack methods that are readily available for purchase, and are well-known to cyber security companies. There are plenty of defenses to stop those attacks.

Next let's turn to vulnerabilities and consequences. A vulnerability analysis is fairly straightforward. Examples could include third party vendors with uncontrolled access, software or hardware no longer supported by the manufacturer, or new devices that have not been fully integrated into the company's cyber defenses.

With respect to consequences, companies need to examine what will happen if certain data or operations are compromised/disrupted/destroyed. Will the damage cause reputational harm, financial loss, physical harm, or merely be inconvenient? The more serious the consequences, the more attention that should be paid to the problem. Wrapping all that together should give a CIO and relevant superiors where resources should go.

It may seem odd that the inherently technological problem of cyberattacks is best countered through a rigorous process and not strictly technological solutions. Yet, given the extraordinary pace of maturation associated with cyberattacks, it makes perfect sense to rely on a process to determine optimal defense strategies. In doing so, companies will not only protect themselves from cyber threats but will also have created a fantastic record of decision-making that will undoubtedly deter litigation. That alone should drive a movement towards process-based defenses.