Banding Together for Cyber Defense

This article was originally published in the *Wall Street Journal's* CIO Journal on May 8, 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.

When discussing how companies can cooperate on cyber security, talk often revolves around information sharing. Yet while there's value in the notion that companies and governments could freely share important threat data such as malware signatures and indicators of compromise, it's not the last word on cooperative cyber defense. Opportunities exist now for CIOs to band together with other internal executives and similarly situated companies in the form of risk-pooling mechanisms to increase their defenses and better mitigate risk.

Through risk pooling, CIOs can work with enterprise risk managers, general counsels, CFOs, and even CEOs to purchase truly worthwhile insurance policies while also establishing hard liability limits and pooling cyber defense resources.

Risk pooling mechanisms come in a number of forms, including "risk purchasing" and "risk retention" groups. Those groups allow collections of companies (usually similarly situated in terms of industry sector) to jointly purchase or create insurance coverage that would otherwise be unavailable or excessively expensive.

The concept of such pools have been around for some time, and discussions are starting with respect to utilizing them in the context of cyber threats. Where a CIO can really take advantage of these mechanisms is to layer in additional risk mitigation tools such as threat information sharing and statutory liability protection. Combining those aspects could lead to a very powerful collective defense tool.

Here's how it can work:

1. A group of similarly situated companies agree to form a risk purchasing or retention group in order to obtain cyber security insurance.

2. The companies agree to use certain security standards or technologies (for instance SANS 20 controls, "detonation chambers", information sharing via dedicated "private clouds", the recent National Institutes of Standards and Technologies voluntary cyber security framework, etc.)

3. The companies then pool their resources to either to jointly purchase an existing cyber insurance policy or to create a pool of insurance that they would maintain.

4. The risk group also agrees to pursue SAFETY Act protections

for the standards it has created and committed to adhering to. For the uninitiated, the SAFETY Act is a law administered by the Department of Homeland Security, under which companies that sell or deploy cyber security products or services can obtain liability protections in the form of either (a) a maximum cap on liability equal to a specific amount of insurance or (b) grants companies the presumption of immediate dismissal of claims arising out of cyber attacks and related to the approved products or services.

5. As part of the agreement, any company that fails to adhere to the security standards will be asked to leave the group at the next renewal period.

What makes this proposal potentially so valuable to the companies involved is the use of the SAFETY Act. The SAFETY Act on top of the insurance pool effectively limits the exposure of the group to the amount of insurance they have purchased, or even a portion thereof. That is because with all the members being covered under the SAFETY Act award, any eligible claim following a cyberattack will be subject to strict liability limits under Federal law. In addition to the maximum awardable damages already mentioned, other types of limits are imposed such as a ban on punitive damages and prejudgment interest.

Further, this arrangement also potentially allows more of the insurance funds to be used for losses the company has directly suffered (damaged equipment, lost data, business interruption, etc.) rather than losses suffered by third parties.

To illustrate, assume a risk group obtains $200 million in insurance, but under the SAFETY Act the most that can be paid to third parties is $100 million. It follows then that the risk group is guaranteed to have at least $100 million available every year to pay for its members first party losses.

CIOs should be interested in this idea because not only does it create a way to gain access to more insurance, but it also potentially achieves a goal many companies are struggling to reach – namely putting some certainty around the losses that could occur following a cyberattack.

The pool arrangement also allows companies to collaborate and establish a baseline of security that each would commit to maintaining, and also allows for regular reviews to determine what security controls need to be adjusted. And again, all of this would fall under the umbrella of a review by the Department of Homeland Security, thereby lending it credence from a Federal agency.

This risk group model gives CIOs and their peers the unique ability to achieve objectives many have been struggling to reach. First, it provides a concrete way to allow for the use of cyber insurance as an incentive to increase security. Second, it gives pool members the ability to establish baseline security requirements that can be blessed by the Federal government with truly tangible benefits – in this case the promise of statutory liability protection in the event of a cyberattack.

The pooling concept gives CIOs an excellent opportunity to take charge of a company's security profile and do so in a way that helps mitigate the potentially enormous liability exposure that would follow a cyberattack. The particular beauty here is that any effective mechanism, whether existing frameworks, controls, or even newly created procedures intended solely for the pool group, could serve to be the baseline for this effort.

Ultimately, CIOs would benefit as they would be viewed as proactive problem solvers, not just implementers of technical solutions. Given the potential legal exposure company executives could face in the event of a successful cyberattack, this approach presents a high chance of a winning scenario for companies and CIOs alike.